Algemene Bestuursdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Moral fitness

Een onderzoek naar de integriteit van de defensieorganisatie ten aanzien van de omgang met commerciële partijen op het gebied van IT



ABDTOPConsult

Dichtbij en onafhankelijk

Colofon
ABDTOPConsult
Muzenstraat 96
2511 WB DEN HAAG

Januari 2016

Koos van der Steenhoven
Marianne Aalbersberg

ABDTOPConsult
De consultants van ABDTOPConsult zijn lid van de topmanagementgroep (TMG) van de Algemene Bestuursdienst. Ze zijn rijksbreed en interbestuurlijk inzetbaar voor interim-opdrachten, projecten en onafhankelijke advisering bij complexe en (politiek) gevoelige zaken.

Inhoudsopgave

Samenvatting

Dit onderzoek gaat over integriteit.

De hoofdvraag die moest worden beantwoord luidt: brengt de manier waarop door het ministerie van Defensie wordt omgegaan met commerciële partijen op het gebied van IT de integriteit van de defensieorganisatie in het geding?

Dit onderzoek is uitgevoerd in opdracht van de minister van Defensie, nadat er enkele vermoedens waren over mogelijke belangenverstrengeling bij de aanschaf van IT. De minister vroeg enkele dossiers tot de bodem uit te zoeken. Dat is gebeurd.

De commissie heeft allereerst het begrip integriteit bestudeerd en nader geëxpliciteerd.

In gesprekken die elkaar in de sneeuwbalmethode opvolgden is met meer dan 150 personen gesproken. Er zijn enkele duizenden bladzijden en mails bestudeerd. Via een speciaal voor het onderzoek geopend meldpunt konden personen met de commissie spreken over de vraag of met commerciële IT-bedrijven op integere wijze zaken wordt gedaan.

1. De commissie heeft, op één geval na, geen aanleiding gehad om specifieke feiten of gedragingen van personen, die strijdig zouden zijn met wet- en regelgeving, onder de aandacht van de secretaris-generaal te brengen. Er zijn geen inbreuken op de integriteit vastgesteld in de zin van corruptie, omkoping, fraude, daadwerkelijke belangenverstrengeling of het ten eigen bate misbruiken of manipuleren van informatie. Er zijn wel onrechtmatigheden vastgesteld, maar deze werden in de normale controlelijn van het departement al eerder aan de orde gesteld.

2. Dit betekent niet dat de conclusie mag worden getrokken dat er weinig tot niets aan de hand is. Op het terrein van IT is in de afgelopen jaren op diverse plekken in de organisatie de schijn van belangenverstrengeling gewekt. Oorzaken voor het onstaan én voortbestaan daarvan moeten worden weggenomen: onduidelijke communicatie, het niet beantwoorden van vragen van medewerkers, en het niet adequaat behandelen van meldingen. Zonder actie op deze punten is de integriteit van de defensieorganisatie in het geding.

3. De hoofdaanbeveling is dat binnen het ministerie van Defensie voortdurende activiteit moet worden georganiseerd op alle plekken in de organisatie om moreel fit te blijven. Dat gaat niet vanzelf. Het vergt dagelijkse oefening. Vandaar de titel: *Moral Fitness*.

4. In een organisatie met ruim 60.000 medewerkers is er elke dag wel wat aan de hand. Dit onderzoek is daarom een momentopname. Maar enkele zaken vragen nu meteen de aandacht.

5. Het beheer van de contracten van Defensie met de IT-leveranciers vertoont gebreken. Veel contracten zijn ook ultimo 2015 niet *up to date*. Dat kan leiden tot het afnemen van diensten op onrechtmatige contracten en dat raakt de integriteit van het handelen van het ministerie. De aanbeveling is om dat systeem zo snel mogelijk te verbeteren. Het probleem is in 2008 ook al aan de Tweede Kamer gemeld en dreigt nu elk jaar terug te komen.

6. Het melden van voorvallen - waaronder integriteitskwesties - is ingewikkeld en de behandeling ervan is niet eenduidig. Waar de behandeling van meldingen niet tot een afronding wordt gebracht komen melders in de kou te staan. Het is aan te bevelen de behandelingsprocessen te standaardiseren en de Centrale Organisatie Integriteit Defensie (COID) uit te breiden met een aantal noodzakelijke taken, zoals de beoordeling van financiële *compliance* en de uitvoering van de klokkenluidersregeling en bemensing van een klokkenluidersloket. COID zou rechtstreeks onder de secretaris-generaal moeten worden gepositioneerd.

7. Het aanbestedingsproces van IT-voorzieningen vergt te veel tijd. Lange aanbestedingsprocedures maken inbreuken op een eerlijke gang van zaken gemakkelijker. Bovendien gaan de ontwikkelingen in de technologie te snel in relatie tot de ingewikkelde en lange duur van de aanbestedingsprocedures. Daardoor loopt het ministerie van Defensie het gevaar achter de feiten aan te hobbelen en niet de meest geavanceerde IT te kunnen inzetten. Aanbestedingsprocedures zouden sterk moeten worden ingekort, inclusief de noodzakelijke goedkeuring van de Tweede Kamer en de betrokkenheid van Bureau ICT Toetsing voor de BIT-procedure. Een experiment is hierbij aan te bevelen.

8. In het reservistenbeleid is sprake van een 'dode hoek'. Die moet worden weggenomen. Er is bij reservisten bijna altijd een dubbel belang: dat van het ministerie van Defensie, maar ook dat van de andere (hoofd-)betrekking. Ook bij zzp-ers. Bij plaatsing en inschakeling van reservisten behoort een professionele match gemaakt te worden en moet strenger worden gekeken naar mogelijke belangenverstrengeling. Het is niet goed uit te leggen dat reservisten tijdens hun passieve militaire status een geactiveerde defensiepas op zak hebben en daarmee vele -soms ook vitale- terreinen van het ministerie kunnen betreden.

9. Leidinggevenden moeten niet te gemakkelijk denken over het effect van hun gesprekken met vertegenwoordigers van IT-bedrijven. De schijn van belangenverstrengeling is gemakkelijk gewekt en dat ontmoedigt de medewerkers die ordentelijk moeten inkopen. Terughoudendheid en transparantie zijn hier geboden.

10. Voorkomen moet worden dat militairen die na het functioneel leeftijdsontslag in dienst treden van bedrijven, aanbestedingsprocedures beïnvloeden. Het is aan te bevelen hier een veel stringentere koers te varen. Het Noorse ministerie van Defensie kan tot voorbeeld strekken.

1 *Moral fitness*: een rapport om de defensieorganisatie moreel fitter te maken

Dit is het rapport van de commissie die onderzoek deed naar de integriteit van de defensieorganisatie waar het gaat om de omgang met commerciële partijen in het domein van de informatietechnologie (IT). Op basis van enkele signalen uit de organisatie vroeg de minister van Defensie om diepgaand onderzoek.

1.1 Veel informatie beschikbaar: wat is nodig om daadwerkelijke verbeteringen te realiseren?

In de loop van het onderzoek, dat uiteindelijk een jaar duurde, bleek dat er een grote hoeveelheid informatie beschikbaar is over het begrip integriteit in het algemeen, over integriteit bij het ministerie van Defensie, over IT bij dit ministerie en ook over integriteit in het IT-domein. Een beknopte samenvatting van al deze stukken die wij maakten voor onze eigen analyse beslaat tegen de 100 pagina's: wet- en regelgeving, achtergronddocumenten, studies, nota's, memo's, brieven, e-mailwisselingen en adviesrapporten. Veel gesprekspartners namen stukken voor ons mee of verwezen ons naar stukken die wij dan weer opvroegen bij het ministerie.

Het viel ons op dat in veel stukken behartenswaardige adviezen staan. Bekende voorbeelden zijn het rapport van de commissie Integriteitszorg Defensie onder leiding van luitenant-generaal b.d. De Veer uit 2011, het rapport van Blauw Research over ongewenste omgangsvormen binnen zes opleidingsinstituten van Defensie uit 2010 en het rapport van de commissie Staal over ongewenst gedrag uit 2006. Een deel van die adviezen is uitgevoerd, maar een deel ook niet. Op zich is dat niet verontrustend: adviezen worden soms ingehaald door nieuwe ontwikkelingen, of opvolging ervan wordt betrokken bij andere verbeteringstrajecten. Wij constateren echter dat er ook aanbevelingen zijn die worden omarmd, maar waarbij het lang duurt eer ze worden opgepakt en tot verbeteringen leiden[1]. Dat riep bij ons de vraag op hoe we de opdrachtgever zo goed mogelijk kunnen helpen om daadwerkelijke verbeteringen te realiseren.

1.2 Integriteit is nooit 'klaar', maar vergt *moral fitness*

Met deze vraag in het achterhoofd hebben wij lang en intensief onderzoek gedaan, om vragen van defensiemedewerkers, leidinggevenden maar ook politici tot op de bodem uit te zoeken. Gedurende het jaar dienden zich nieuwe zaken aan, die ook moesten worden onderzocht. Tot laat in december benaderden mensen ons voor een gesprek. De bodem kwam wel in zicht, maar werd niet bereikt.

[1] Een pregnant voorbeeld dat in dit rapport aan de orde komt gaat over adviezen over contractbeheer. Een ander voorbeeld is de trage uitvoering van voornemens om de meldsystematiek te verbeteren. Onder meer in

Gaandeweg kwamen wij tot de conclusie dat er bij integriteitsonderzoek als dit nooit een definitieve streep kan worden getrokken. Nadenken over integriteit is nooit klaar, maar vergt constante aandacht en actie. Alleen zo kan een organisatie fit blijven op integriteitsgebied: er is *moral fitness* nodig. Wij ontlenen deze term aan prof. dr. D.E.M. Verweij, hoogleraar militaire ethiek aan de Nederlandse Defensie Academie en bijzonder hoogleraar normatieve en beleidsmatige dilemma's van mulitalerale vredesoperaties aan de Radboud Universiteit. Zij is co-auteur van het artikel '*Moral fitness for peace operations*', een interessant betoog over het belang van *moral fitness* en over de manier waarop mensen moreel fit kunnen worden en blijven. Hoewel het artikel vooral geschreven is vanuit het gezichtspunt van deelname aan internationale missies, is het onzes inziens breed bruikbaar voor het ministerie van Defensie[2].

1.3 Aanbevelingen voor *moral fitness*

Waar moeten de fitnessoefeningen zich dan op richten? In de loop van de interviews maakten wij talloze aantekeningen over verbeterpunten. Ook onze gesprekspartners kwamen met veel suggesties en ideeën. Als we die allemaal op een rijtje zouden zetten, dan hadden we een enorm dik rapport afgeleverd. Met nieuwe regels, nieuwe overleggen. Die dan weer bovenop de bestaande hoeveelheid regels en overleggen zouden komen. We raakten er echter steeds meer van overtuigd dat onze bevindingen vragen om andersoortige aanbevelingen. Aanbevelingen die gaan over de onderliggende oorzaken van integriteitschendingen en integriteitsrisico's.

Onze hoofdaanbeveling is om te blijven oefenen met integriteit.

Oefenen met integriteit is *moral fitness.* Denk aan dilemmatrainingen, moreel beraad, casusstudies, personeelsgesprekken, risicoanalyses. Die oefeningen moeten rekening houden met het feit dat integriteitszaken, vermoedens van integriteitschendingen en andere meldingen nooit gereduceerd mogen worden tot een juridische kwestie of een dichotome goed/fout-vraag. Ze moeten rekening houden met bestuurlijke en ethische aspecten van integriteit. Het is belangrijk te beseffen dat integriteitsvragen er altijd zullen zijn en blijven, en dat een goed integriteitsbeleid begint bij transparant communiceren en adequaat reageren op vragen en zorgen die leven bij mensen in de organisatie.

> ***"Like physical fitness, moral fitness also implies regular training in order to stay in shape. Moral fitness is not something that can be won once and for all; it requires a continuous reflection on the values and norms one lives by and is confronted with, reflection on what to do and how and why it should be done."***
> (bron: '*Moral fitness for peace operations*', R. Richardson, D. Verweij en D. Winslow)

1.4 Openhartige en soms confronterende gesprekken

Wij bedanken iedereen die met ons heeft gesproken voor de openhartige manier waarop dat gebeurde. Vaak kwamen gesprekspartners tijdens het gesprek of daarna nog met suggesties voor andere gesprekken of voor stukken die we moesten lezen. Dat toont de enorme betrokkenheid van velen. Wij bedanken ook iedereen die het afgelopen jaar stukken voor ons heeft opgezocht en archieven heeft doorgespit, niet alleen op het ministerie maar ook op enkele ambassades.

---

[2] '*Moral fitness for peace operations*' van R. Richardson, D. Verweij en D. Winslow, *Journal of Political and Military Sociology, Summer 2004*. Het artikel is integraal opgenomen aan het eind van dit rapport.

Onze gesprekken waren soms ook lastig, pijnlijk en confronterend voor onze gesprekspartners. Mensen wonden zich op, er vielen stiltes, er waren tranen. Verhalen gingen soms over situaties van vele jaren geleden: het zat onze gesprekspartners nog steeds dwars. Het is met deze emoties in het achterhoofd dat wij het onderzoek zo grondig hebben uitgevoerd. Vragen en vermoedens hebben wij steeds uitgezocht. Uit reacties op de terugkoppeling die wij onze gesprekspartners daarover gaven, bleek dat onze gesprekspartners zich gehoord voelden. Zij waren blij dat hun vragen werden beantwoord, en ook opgelucht als wij konden terugkoppelen dat er geen sprake was geweest van zaken als fraude of belangenverstrengeling.

2 Aanleiding, opdracht, definitie van IT en leeswijzer

2.1 Aanleiding

In de zomer en het najaar van 2014 kreeg de minister van Defensie signalen, onder andere via televisieprogramma Zembla, dat er in de omgang tussen het ministerie van Defensie en commerciële partijen in het domein van de IT mogelijk was gehandeld in strijd met wet- en regelgeving. Een interne ambtelijke commissie die de signalen onderzocht, adviseerde om nader onderzoek te doen[3]. De minister van Defensie gaf daarop opdracht om grondig onafhankelijk onderzoek te laten doen. De politieke en ambtelijke leiding vond de signalen die hen bereikten zorgelijk en vroeg om deze en mogelijke andere kwesties tot op de bodem uit te zoeken[4].

2.2 Opdracht

De centrale onderzoeksvraag in dit onderzoek was:

Brengt de manier waarop door het ministerie van Defensie wordt omgegaan met commerciële partijen op het gebied van IT de integriteit van de defensieorganisatie in het geding? [5]

---

[3] Het ministerie van Defensie had behoefte aan nader inzicht in:

- de bedrijven die het ministerie inhuurt op het gebied van IT en de mogelijke afhankelijkheidsrelaties die er bestaan met deze bedrijven en de (gewenste en ongewenste) consequenties daarvan;
- onregelmatigheden die mogelijk hebben plaatsgevonden bij aanbestedingen van IT-goederen en –dienstverlening;
- (onwenselijke) banden die er mogelijk bestaan tussen commerciële partijen die zaken doen met het ministerie op IT-gebied en individuele functionarissen van Defensie en de invloed van deze banden op genomen beslissingen.

[4] De minister van Defensie gaf op vragen van Kamerleden Knops en Van Dijk aan: "*De heer Van Dijk vroeg ook nog naar fraude als gevolg van ontbrekende controle. We hebben de commissie-Van der Steenhoven. De heer Knops vroeg er ook nog naar. Uiteindelijk ben ik naar aanleiding van de vraag van de heer Knops daartoe overgegaan. We hebben eerst oppervlakkig onderzoek gedaan. We hebben vervolgens vastgesteld of dit voldoende aanleiding geeft in combinatie met de uitzending van Zembla en ga zo maar door, om een enorme verdiepingsslag te maken. Het antwoord op die vraag was ja. Wij hebben Koos van der Steenhoven daarvoor aangenomen. Als er nu meldingen binnenkomen, worden die meegenomen. Het stopt dus niet. Als een melding voldoende substantieel is om tot aangifte over te gaan, doen we dat. Ik kan echt nog niet zeggen of het daarop zal uitdraaien, dus of er daadwerkelijk sprake is geweest van fraude, of grenzen zijn opgezocht of dat daadwerkelijk strafrechtelijke grenzen zijn overschreden. Daar kijkt de commissie-Van der Steenhoven voor ons naar. Zij is nu bezig met deskresearch. Dat is een aanzienlijke exercitie, want een melding bestaat uit een hoeveelheid documentatie en mails die daaraan ten grondslag liggen. Ik verwacht dat de commissie uiterlijk op 1 februari aanstaande een eerste tussenrapportage levert. Vanzelfsprekend zal ik die ook met de leden delen. Die tussenrapportage zal ook licht laten schijnen op de vervolgplanning van het onderzoek*." (Verslag van een Algemeen Overleg over Informatievoorziening en ICT bij Defensie, 5 november 2014, kamerstuk 31 125 nr 51)

[5] Een medewerker van het ministerie van Defensie wees ons vroeg in het onderzoek op een taalkundige fout in onze onderzoeksopdracht. Er worden twee uitdrukkingen door elkaar gebruikt, zo schreef hij: 'in gevaar brengen' en 'in het geding zijn'. Beter was geweest: *Is bij de manier waarop het ministerie van Defensie omgaat met commerciële partijen op het gebied van IT de integriteit van de defensieorganisatie in het geding?* Wij drukken hier toch de oorspronkelijke onderzoeksopdracht af omdat hij zo in onze instellingsbeschikking staat.

Op basis van een kort vooronderzoek hebben wij – in overleg met de opdrachtgever - een aantal deelvragen geformuleerd die bij de beantwoording van de centrale vraag in elk geval aan de orde zouden moeten komen:

1. *Wordt er door medewerkers van het ministerie van Defensie, of door medewerkers die (extern) door Defensie zijn ingehuurd, in de omgang met commerciële partijen op het gebied van IT gehandeld in strijd met wet- en (interne) regelgeving?*
2. *In hoeverre kan er voordeel zijn voor medewerkers en/of commerciële partijen bij een dergelijke handelswijze?*
3. *Wat zijn de achterliggende oorzaken van de omgangswijze?*
4. *Is er sprake van een praktijk waarbij binnen het IT-domein nauwe banden met commerciële partijen ontstaan, bijvoorbeeld op het gebied van contractvorming bij en de positionering van extern ingehuurde medewerkers?*
5. *In hoeverre worden daarbij ongewenste beïnvloedingsstrategieën gehanteerd door commerciële partijen in de IT-sector?*

Het ministerie van Defensie vroeg om ook aanbevelingen te doen naar aanleiding van de bevindingen en de beantwoording van de onderzoeksvragen.

Het onderzoek gaat over de periode 2010 tot en met 2014. Zoals beschreven in de instellingsbeschikking konden wij relevante signalen die buiten deze periode vallen ook betrekken bij het onderzoek. Dat hebben wij ook gedaan. Reeds vroeg in het onderzoek kregen wij signalen dat ook gebeurtenissen uit de periode 2000 tot 2010 door ons onderzocht moesten worden. Het gaat dan vooral om gebeurtenissen rond de langdurige discussie over het al dan niet *sourcen* van onderdelen van het ministerie.

2.3 Definitie van IT

Wij hanteren een brede definitie van IT:

> **IT is het vastleggen of verwerken van gegevens en informatie via (computer)technologie**
> (bron: www.encyclo.nl)

Zo beschouwd is IT te vinden op veel plekken en in bijna alle werkprocessen van het ministerie van Defensie.

2.4 Leeswijzer

In hoofdstuk drie gaan wij nader in op het begrip integriteit en op onze werkwijze. In hoofdstuk vier presenteren wij de voornaamste bevindingen en conclusies. Op basis daarvan beantwoorden wij in hoofdstuk vijf de hoofdvraag en de deelvragen van dit onderzoek. In hoofdstuk zes doen wij aanbevelingen, en in hoofdstuk zeven blikken we kort terug op het onderzoek.

3 Het begrip integriteit en onze werkwijze

3.1 Integriteit

Uit onze gesprekken en uit de beschikbare literatuur blijkt dat er diverse invalshoeken zijn om naar het begrip integriteit te kijken. Bovendien veranderde de kijk op integriteit in de loop van de voorbije decennia. Naast een filosofische en ethische invalshoek, vooral gericht op het individu, kreeg het begrip integriteit ook een bestuurlijk en juridisch perspectief, mede gericht op de organisatie waarin een individu functioneert. Onderzoek naar integriteit kan dan ook nooit eendimensionaal zijn. Het gaat om toetsen van gedragingen aan wet- en regelgeving, maar ook bestuurlijke en meer ethisch-morele vragen moeten aan de orde komen. En daarbij gaat het niet alleen om individuen, maar ook om de organisaties waarin zij werken én de maatschappij waarin die organisaties hun functie vervullen[6].

In dit onderzoek gebruiken wij de Definitie van integriteit die het ministerie van Defensie zelf hanteert:

> **Integriteit is respectvol met elkaar (en met anderen) omgaan, waarbij rekening wordt gehouden met de gerechtvaardigde belangen en wensen van alle betrokkenen.**
> (bron: SG Aanwijzing 984 Uitvoering van het integriteitsbeleid Defensie)

Dit is een brede definitie, waarin vooral de inschatting van het individu voorop staat: hoe ga jij met anderen om? Om enig houvast te hebben in het brede veld van integriteit gebruikten wij bij ons onderzoek daarnaast een verdeling in negen soorten integriteitschendingen, ontleend aan Prof. dr. J.H.J. van de Heuvel in 'Integriteit. Integriteitsbeleid in Nederland' (J.H.J. van den Heuvel, L.W.J.C. Huberts en E.R. Muller, 2012):

- corruptie of omkoping;
- fraude of verduistering;
- beloften of giften waar geen tegenprestatie voor wordt gevraagd;
- belangenverstrengeling, in het bijzonder het vermengen van publieke met private belangen;
- nepotisme door het bevoordelen van familieleden, vrienden of relaties;
- het hebben van onverenigbare nevenfuncties of nevenactiviteiten;
- het te eigen bate misbruiken of manipuleren van informatie;
- het uitoefenen van intimidatie of het scheppen van angstcultuur;
- misbruik maken van bevoegdheden.

Bij het voeren van gesprekken, het bestuderen van stukken en het onderzoeken van casuïstiek hebben wij onszelf steeds de vraag gesteld of defensiemedewerkers handelden conform de wet- en regelgeving, of zij handelden naar de definitie van integriteit die het ministerie gebruikt en of zich in de relatie met commerciële partijen één of meer van de negen integriteitschendingen voordeed. Ook keken wij – de bestuurskundige invalshoek – naar de organisatie als geheel: bevordert de defensieorganisatie dat medewerkers kunnen handelen conform wet- en regelgeving, handelt de organisatie naar de eigen definitie van integriteit? Is de organisatie zo ingericht dat de negen integriteitschendingen worden voorkomen? Deze toetsvragen hielpen ons een brede blik te houden, op zoek naar structuren en onderliggende oorzaken.

---

[6] Zie voor een overzicht van ontwikkelingen de bijdrage van Prof. dr. G.H. Addink in de bundel '*Integriteit. Integriteitsbeleid in Nederland*' (J.H.J. van den Heuvel, L.W.J.C. Huberts en E.R. Muller, 2012).

3.2 Werkwijze: grondig onderzoek gebaseerd op verhalen uit gesprekken

De opdracht die wij kregen bevat de geformuleerde onderzoeksvraag en de deelvragen, maar wij kregen ook de vraag om een enkele casus tot de bodem toe uit te zoeken. De achtergrond van die vraag was duidelijk: de signalen over mogelijke misstanden bleken al meerdere jaren te leven in de organisatie. Onderzoeken hadden tot dusver weinig concrete aanwijzingen opgeleverd dat er zaken mis waren, maar de signalen bleven terugkomen. De leiding van het ministerie vroeg dus om een grondig onderzoek. En uit de korte beschouwing over integriteit hierboven blijkt al dat niet gewerkt zou moeten worden met een simpele checklist of goed/fout-vragen.

Wij kozen daarom voor een onderzoeksmethode waarbij de verhalen die gesprekspartners vertellen een belangrijke rol spelen. Deze onderzoeksmethode wordt vaker gebruikt bij weerbarstige, complexe onderwerpen en bij minder concrete thematiek waarbij op voorhand nog slecht te voorspellen is wat het zwaartepunt van het onderzoek zal zijn en wat het onderzoek op zal leveren. Zo denken wij een stap verder te zijn gekomen dan integriteitsonderzoek waarbij louter de vraag aan de orde is of er corruptie of fraude heeft plaatsgevonden. Er zijn drie onderzoekslijnen te onderscheiden in ons onderzoek.

Eerste onderzoekslijn: gesprekken volgens de sneeuwbalmethode

De eerste en meest omvangrijke onderzoekslijn was het voeren van een grote hoeveelheid gesprekken volgens de sneeuwbalmethode. De serie gesprekken startte begin 2015 met enkele gesprekken met mensen die signalen hadden gegeven over mogelijke misstanden rond verwerving en contractering in het IT-domein. Uit die gesprekken kwamen namen naar voren van mensen die vervolgens door ons werden uitgenodigd voor een gesprek. En zo steeds verder. Wij hebben in totaal ruim 150 personen gesproken. Gesprekpartners kwamen uit alle delen van de defensieorganisatie. Ook spraken wij met enkele personen die bij IT-bedrijven werken, met TNO en de Nationale Politie, en met een aantal wetenschappers.

De gesprekken hadden een open en vertrouwelijk karakter. Met alle gesprekspartners is afgesproken dat er niet zou worden geciteerd uit het gesprek. Om het gesprek zo open mogelijk te kunnen voeren zijn er geen verslagen gemaakt. Aan het eind van elk gesprek werd gevraagd of er nog zaken waren die wij niet aan de orde hadden gesteld, maar die volgens de gesprekspartner wel van belang waren voor het onderzoek.

Tweede onderzoekslijn: bestuderen van stukken

De tweede onderzoekslijn betrof het bestuderen van een grote hoeveelheid stukken: wet- en regelgeving, interne nota's, memo's, studies, dossiers, rapporten en emails, externe adviesrapporten, achtergrondliteratuur, informatie van internet en stukken die ons werden aangereikt door defensieattachés. Er zijn duizenden pagina's stukken bestudeerd.

Derde onderzoekslijn: meldpunt

Hoewel de sneeuwbalmethode er voor zorgt dat de onderzoeksblik steeds ruimer wordt, viel niet uit te sluiten dat wij zaken zouden missen die wel van belang waren voor ons onderzoek. Daarom hebben wij een derde onderzoekslijn gebruikt in de vorm van een meldpunt voor defensiemedewerkers. Wij hebben een e-mailadres geopend (ITDEF-integriteit@rijksoverheid.nl) buiten het e-mailsysteem van het ministerie van Defensie waar medewerkers zich konden melden als zij iets met ons wilden bespreken. Daarvan heeft een aantal mensen gebruik gemaakt. Dit leverde nieuwe verhalen, nieuwe casuïstiek op, die wij vervolgens onderzochten op de manier die hierboven is beschreven.

Naast deze drie onderzoekslijnen hebben wij een beperkte internationale benchmark uitgevoerd. De hoofdvraag daarbij was of er landen zijn waar Nederland van kan leren. Te denken valt aan de samenwerking met de markt, het reservistenbeleid, integriteitsbeleid en het opvolgen van integriteitsmeldingen. Op enkele plekken in dit rapport geven wij voorbeelden uit andere landen.

3.3 Hoe kan dit rapport zo dun zijn: waar is de bewijslast?

Op basis van het voorgaande zal duidelijk zijn dat wij in de loop van dit lange en grondige onderzoek een aanzienlijke hoeveelheid informatie hebben verzameld. En sommige lezers verwachten daarom wellicht een heel dik rapport vol bewijslast, verslagen, processen verbaal, uitvoerige casuïstiek en cijfermatige onderbouwingen. Wij hebben daar niet voor gekozen. Wij waren geen rechercheteam en daar was ook geen aanleiding toe.

Eerder gaven wij al aan dat wij ons vroeg in het onderzoek voornamen om vooral te zoeken naar mogelijkheden om zaken op te lossen en daadwerkelijke verbeteringen te realiseren. Immers, eerdere onderzoeken naar de signalen uit de organisatie hadden weinig concrete aanwijzingen opgeleverd dat er zaken mis waren, maar de signalen bleven terugkomen. Wij hebben gekozen voor een opbouw van het rapport en voor een presentatie van onze bevindingen die daar dienstbaar aan is. Wij presenteren bevindingen in het volgende hoofdstuk als korte beschrijvingen van gebeurtenissen. Casuïstiek wordt in deze beschrijvingen veelal gebundeld en geanonimiseerd. Zo ontstijgt de analyse het niveau van incidenten of individuele casuïstiek en ligt de nadruk op achterliggende oorzaken en terugkerende patronen die verbetering in de weg staan.

4 Bevindingen en conclusies, samengevat in drie thema's

In dit hoofdstuk presenteren wij een samenvatting van de bevindingen uit de gesprekken en het bestudeerde schriftelijk materiaal. Zoals in het vorige hoofdstuk aangegeven vormen verhalen over integriteit en de aankoop van IT het hart van deze studie. De documenten die wij hebben bestudeerd, en de inhoud van de gesprekken die wij voerden, leverden een drietal dominante thema's op. Wij hebben alle belangrijke elementen rond de onderzoeksvraag kunnen ordenen aan de hand van deze drie thema's. Het eerste dominante thema betreft het beheer van de contracten en de manier waarop IT-diensten en goederen worden verworven. Het tweede dominante thema is de manier waarop medewerkers van het ministerie van Defensie omgaan met marktpartijen. En het derde dominante thema gaat over de manier waarop medewerkers vermoedens van integriteitschendingen kunnen melden en de wijze waarop die meldingen vervolgens worden behandeld cq. afgehandeld.

Wij werken de drie dominante thema's in dit hoofdstuk verder uit met bevindingen uit de gesprekken en de bestudeerde documenten. Dat doen wij in losse tekstblokken waarin we casuïstiek beschrijven. Waar relevant, vermelden wij in die tekstblokken ook de constateringen en conclusies die ons onderzoek naar de betreffende casus opleverde. Wij besluiten elk van de drie thema's met een aantal overkoepelende conclusies. Op basis daarvan beantwoorden wij in hoofdstuk vijf de hoofdvraag en de deelvragen van dit onderzoek. In hoofdstuk zes doen wij een hoofdaanbeveling en enkele aanbevelingen voor de drie thema's.

4.1 Eerste thema: verwerven en contractbeheer

Lange discussie over wel of niet sourcen van IT leidt tot vermoedens van belangenverstrengeling

Vanaf midden jaren '90 wordt gesproken over de mogelijke *(out)sourcing* van de IT van het ministerie van Defensie. In de langslepende discussie wordt een aantal keer het besluit genomen om te *sourcen* en dat besluit wordt ook een aantal keer herroepen. Medewerkers stellen vragen over gevolgen van de voorgenomen *sourcing* voor de staatsveiligheid. Deze vragen worden niet zodanig beantwoord dat betrokkenen gerustgesteld zijn. Integendeel, zij zien zaken die initiële vermoedens van belangenverstrengeling alleen maar aanwakkeren: vragen over de veiligheid van de IT-voorzieningen worden niet beantwoord, er zijn voor hen onverklaarbare wendingen in de besluitvorming, leidinggevenden stellen stukken op, zónder beweringen en cijfers intern te laten toetsen, er is een zware lobby vanuit een aantal IT-bedrijven – een accounthouder van één van de bedrijven schrijft zelfs een beleidsstuk dat als intern document behandeld wordt –, er zijn plotselinge personele wisselingen aan de top van het ministerie en er zijn geruchten over torenhoge bindingspremies[7]. Al met al ontstaat bij betrokkenen het beeld dat hoofdrolspelers – soms zelf afkomstig van een bedrijf - een persoonlijk of commercieel belang hadden bij het nemen van beslissingen.

Wij hebben deze vermoedens diepgravend onderzocht en in vele gesprekken aan de orde gesteld. Wij hebben niet aan kunnen tonen dat de vermoedens juist waren. Wel kende bijna iedereen die wij in dit verband spraken de geruchten. Vragen over de gevolgen van veranderingen voor personeel en voor de staatsveiligheid werden niet goed beantwoord, hoogoplopende ruzies onder leidinggevenden schiepen een angstcultuur. De vermoedens en geruchten leefden bij velen in de periode 2000 – 2014. Dat is een lange tijd. Overigens is in recente stukken over de vernieuwing van de IT bepaald dat cruciale en vitale IT-voorzieningen van Defensie niet meer zullen worden uitbesteed.

[7] De bindingspremies zijn door ons onderzocht. Ze waren in overeenstemming met de geldende regelgeving.

Onregelmatigheden bij de inkoop van IT

In enkele dossiers troffen wij onregelmatigheden aan die in de afgelopen jaren hebben plaatsgevonden bij de inkoop van IT. Het ging daarbij om zaken als tussentijdse contractvernieuwing binnen projecten en uitvraag van diensten van externe medewerkers die niet onder het oorspronkelijke contract vielen. Deze onregelmatigheden werden door defensiemedewerkers in de controlelijn van het ministerie aan de orde gesteld: controllers, auditors, inkoopverantwoordelijken. Er is geen sprake geweest van aangiften of van meldingen bij het OM.

Een aantal mensen sprak met ons over externe projectleiders die vaak lange tijd sleutelposities innamen in langlopende IT-projecten als SPEER, MULAN, Defensiepas. Er werden vermoedens geuit dat die externe projectleiders zelf weer externen in konden huren van hun eigen bedrijf, of zelfs dat zij hun eigen contract konden verlengen. We kregen ook een casus aangereikt over een externe kracht die langdurig werd ingehuurd op steeds verschillende projecten, door steeds dezelfde defensiemedewerker. Mensen die dergelijke zaken met ons bespraken waren bang dat commerciële belangen prevaleerden boven defensiebelangen.

Uit bestudering van de regelgeving en de dossiers blijkt dat projectleiders, intern en extern, in de regel verantwoordelijk zijn voor het maken van een behoeftestelling voor inhuur van tijdelijke medewerkers. De daadwerkelijke inkoop van externe inhuur gebeurt door de inkooporganisatie. Projectleiders spelen in de inkoopfase een rol bij de beoordeling van CV's. Bij een aantal projecten zagen wij dat er vanuit de inkooporganisatie en de interne controlfuncties vragen werden gesteld, bijvoorbeeld over het steeds opnieuw inhuren van dezelfde persoon. Betrokkenen wezen op de risico's die langdurige inhuur met zich mee zou brengen. Als reactie op dergelijke berichten werd er soms behoorlijke druk uitgeoefend op de inkopers en controllers om mee te werken en 'niet moeilijk te doen' om de voortgang van het project niet in gevaar te brengen.

Een voorbeeld is de gang van zaken bij de uitvoering van een groot IT-project. Al vroeg in het proces kwamen er vragen of de externe projectleider niet teveel invloed had op het inhuren van projectmedewerkers. Hij bleek verregaande tekenbevoegdheden te hebben gekregen en was contracten aangegaan met het bedrijf waar hij zelf ook werkte. De auditdienst deed onderzoek en constateerde dat er onder druk – het was een vitaal project dat op dat moment niet goed liep – besloten werd om soepeler met de regels om te gaan. Er volgde een discussie tussen een aantal organisatieonderdelen die enkele jaren (!) duurde en uiteindelijk niet van een conclusie werd voorzien.

Ook steeds doorgaande discussies over techniek leiden tot vermoedens van belangenverstrengeling

In de bestudeerde stukken kwamen wij discussies tegen tussen collega's over technologische keuzes. Ook nadat een besluit was genomen over de toe te passen techniek of de te gebruiken software gingen interne discussies gewoon door, vaak samenhangend met persoonlijke voorkeuren. Een voorbeeld is de doorlopende discussie over SAP versus SGA/BPM-oplossingen. De leiding tolereerde dergelijke steeds opborrelende discussies. Dat riep, zo bleek uit onze gesprekken, bij collega's vermoedens op dat de betreffende medewerker persoonlijk gewin zou hebben bij implementatie van dergelijke oplossingen. Dat gold eens te meer als de persoon in kwestie warme contacten onderhield met bedrijven die dergelijke oplossingen aanboden. Wij hebben geen bewijzen gevonden van daadwerkelijke belangenverstrengeling. Eerder lijkt het te gaan om bevlogen medewerkers die oplossingen bleven zoeken in de complexe en soms moeizaam verlopende IT-projecten. Wij kunnen ons niettemin goed voorstellen dat dergelijk gedrag, namelijk onduidelijke communicatie en voortgaande discussie over iets dat na lange tijd wel van een besluit werd voorzien, vermoedens van belangenverstrengeling opriep. Overigens is door de nieuwe leiding van JIVC en OPS (zie box op de volgende pagina) aangegeven dat besluiten over technologische keuzes alleen door hen worden genomen. Die duidelijkheid kan helpen om genoemde vermoedens in de toekomst te vermijden.

JIVC en OPS

Vanwege de aard van de materie hebben wij veel onderzoek gedaan naar zaken die speelden of spelen op het terrein van de twee organisaties die samen verantwoordelijk zijn voor een groot deel van de IT van het ministerie: het Joint IV Commando (JIVC) en Operations (OPS), beide onderdeel van de Defensie Materieel Organisatie (DMO). Het is bekend dat zich in de afgelopen jaren diverse problemen hebben voorgedaan binnen en tussen deze twee organisatieonderdelen[8]. Sinds najaar 2014 hebben de organisatieonderdelen een geheel nieuw managementteam. Wij constateren dat de huidige leidinggevenden zichtbaar werk maken van de onderlinge samenwerking tussen de organisatieonderdelen. In goed overleg worden er heel wat (technische) knopen doorgehakt. Als er zaken spelen, zoekt men elkaar op om die te bespreken en tot oplossing te brengen. Binnen DMO als geheel is er systematische aandacht voor het onderwerp integriteit.

Er is echter nog steeds onrust en wantrouwen onder het personeel. Dat heeft ook te maken met twijfels over de baanzekerheid bij het personeel. Het zal tijd en forse inspanningen vergen om zaken die al jaren niet goed liepen ten goede te keren. Ruimhartige, heldere en empathische communicatie is daarbij van groot belang, zeker nu nieuwe reorganisaties in het kader van de vernieuwing van de IT van het ministerie voor de deur staan.

Onrechtmatigheden bij het contractbeheer op het terrein van IT in 2008

In 2008 deden zich onrechtmatigheden voor bij de inhuur van externe medewerkers op het terrein van IT. In de controle op de jaarstukken hebben de auditdienst en ook de Algemene Rekenkamer melding gemaakt van onrechtmatigheden en onzekerheden voor een totaal bedrag ter grootte van 68 miljoen euro. Zo werden er externe medewerkers ingehuurd, terwijl de (mantel)contracten al waren verlopen. Naar aanleiding hiervan is indertijd een ambtelijke werkgroep opgericht. In 2009 werden achterstanden in het contractbeheer ingelopen en zijn werkprocessen opnieuw ingericht om herhaling te voorkomen. Vermoedens die aan ons werden gemeld, dat deze onrechtmatigheden onder het tapijt waren geveegd, blijken niet juist. De gang van zaken is uit gesprekken en op basis van archiefmateriaal goed te achterhalen en te verklaren.

Onregelmatigheden bij contractbeheer op het terrein van IT doen zich ook in de afgelopen twee jaar voor

Bovenstaande problemen zijn na 2008 niet opgelost. Aanbevelingen van de auditdienst om een centraal contractenregister in te richten worden spaarzaam en verbrokkeld over de defensieorganisatie opgevolgd. Ook in 2014 en in 2015 zijn er problemen met het contractbeheer op het terrein van IT. In beide jaren moeten er wederom forse inhaalslagen worden gemaakt om het beheer op orde te krijgen.

[8] Zie onder meer *ICT/IV Review. Assessment of the Current State of the Ministry of Defence ICT/IV Organisation, Governance and Supporting Infrastructure* (Forrester, 2014).

Het ministerie heeft een regelmatig optredende rechtmatigheidsvraag te verwerken doordat veel contracten waarop IT-diensten worden ingekocht niet tijdig worden verlengd. Contracten zijn verlopen of dreigen te verlopen terwijl de dienstverlening nog doorgaat, of zonder dat duidelijk is of er nog behoefte is aan verdere dienstverlening. Eind 2015 verkeert 37% van de contracten in beheer bij DMO/JIVC en DMO/OPS in de oranje (33%) of rode (4%) zone. Dat betekent dat er onzekerheid bestaat over de rechtmatigheid van deze contracten[9]. Desgevraagd blijft het onhelder wie daarvoor verantwoordelijk is. Organisatieonderdelen wijzen naar elkaar: de behoeftesteller, de vraag-aanbodorganisatie, de inkooporganisatie.

Langdurige aanbestedingen veroorzaken integriteitsrisico's

De door ons onderzochte aanbestedingen duurden zonder uitzondering erg lang. Een in het oogspringend voorbeeld is het Verbeterd Operationeel Soldaat Systeem (VOSS) waarvan de aanbesteding acht jaar vergde. Door tussentijdse wijzigingen in de prioriteiten – vaak ook vanwege de bezuinigingen die op de IT-projecten neerslaan – wordt de vaart uit de projecten gehaald. Verder is het aanbestedingsproces ingewikkeld. Het kent vele stappen en controlemomenten, deels volgend uit externe regelgeving, maar ook volgend uit eigen, extra regels van het ministerie van Defensie.

Wij onderzochten een aanbesteding die niet alleen lang duurde maar ook rommelig verliep en door de complexe dossieropbouw lastig te reconstrueren was. Wij zagen in dit dossier dat de rubricering – en daarmee de werkwijze - na de start van de aanbesteding werd gewijzigd, zonder adequate informatievoorziening aan alle betrokken partijen.

Niet alleen grote aanbestedingen duren lang, ook kleine. Voor de tijdelijke inhuur van een externe medewerker troffen wij een proces aan, waarin minstens tien handtekeningen moesten worden gezet. Waaronder drie van dezelfde persoon, op diverse momenten.

In het IT-domein geldt dat de markt zich zeer snel ontwikkelt. Er komen steeds sneller nieuwe producten beschikbaar. Wat vandaag *up-to-standard* is, is morgen achterhaald. Dat stelt onzes inziens extra eisen aan het tempo van aanbesteden. Er bestaat geen apart aanbestedingsproces voor IT-projecten. Er is aarzeling in de verwervingsketen om vernieuwende en snellere verwervingsstrategieën te hanteren. Het verwervingsproces is zo ingericht dat behoeftesteller en verwerver ver uit elkaar staan. Verantwoordelijkheden zijn versnipperd. Behoeftestellers spreken over een black box, waar soms zelfs een gewijzigd program van eisen uitrolt, zónder dat zij dat weten. Behoeftestellers kennen soms de inhoud van contracten niet.

Lange aanbestedingstrajecten zijn inefficiënt, maar roepen ook integriteitsrisico's op. Ze maken inbreuken op een eerlijke gang van zaken gemakkelijker. Medewerkers proberen – zeker bij operationeel belang – processen te versnellen. Er ontstaat druk om de regels niet (helemaal) te volgen. Zo zagen wij mails waarin vragen werden gesteld over langjarige inhuur van externe medewerkers. Die vragen werden weggespeeld met een kort antwoord: "We zitten in een tijdsklem, het moet nu maar even zo."

[9] Het gaat om bijna 500 contracten. Er zijn ook contracten op het terrein van IT in beheer bij andere organisatieonderdelen.

Ook in andere landen problemen met IT-projecten en aanbesteden
Wij hebben geen *best practice* kunnen vinden op het gebied van aanbesteden. Als het gaat om het tempo van aanbesteden hoorden wij verhalen die vergelijkbaar zijn met de situatie in Nederland. Zo is in de **Verenigde Staten** een discussie gaande over het versnellen van aanbestedingen en over een betere aansluiting tussen behoeftesteller en verwerver. De meest recente ontwikkeling is dat een deel van de centralisering van de inkoop (vergelijkbaar met de situatie in Nederland) wordt teruggedraaid ten gunste van inkoop door afzonderlijke krijgsmachtdelen. Overigens kan Nederland zeker leren van de Verenigde Staten op het gebied van opleidingen in aanbesteden. De krijgsmacht heeft een aparte *Acquisition University* waar alle inkopers en vele anderen een opleiding krijgen met onder meer praktijksimulaties.

In **Frankrijk** kampte de krijgsmacht in 2013 met de gevolgen van een slecht uitgevoerd IT-project voor de salarisadministratie. Lonen werden niet of te laat betaald en er werden verkeerde bedragen overgemaakt. Vanwege de omvang en de impact op de medewerkers werd het project onderwerp van publieke discussie. Naar zeggen van de Franse Rekenkamer bedroegen de extra projectkosten 480 miljoen euro. Uiteindelijk werd eind 2014 besloten een geheel nieuw systeem in te voeren.

Conclusies over verwerven en contractbeheer:

Niemand is verantwoordelijk voor het geheel

Er zijn veel regels. Dat is verklaarbaar uit rechtmatigheidsproblemen in het verleden, en uit de voorschriften die voortvloeien uit aanbestedingswetgeving. Maar al met al is de inkoopketen nu zo georganiseerd, dat veel organisatieonderdelen over een klein stukje gaan. Verantwoordelijkheden liggen versnipperd in de organisatie, waardoor organisatieonderdelen naar elkaar kunnen wijzen als er iets mis gaat. Niemand is verantwoordelijk voor het geheel. Doorlooptijden zijn lang, mede door de vele stapjes in het aanbestedings- en verwervingsproces. Het handboek verwerving is veel te ingewikkeld met ruim 300 pagina’s en nog eens bijna 300 pagina’s bijlagen. De behoeftesteller, die het meest baat heeft bij inzicht in bijvoorbeeld de einddatum van een contract heeft een te kleine rol bij het verlengen van contracten of het uitvoeren van een nieuwe aanbesteding. Er lijkt geen standaardprocedure te zijn hoe moet worden gehandeld bij gerubriceerde aanbestedingen.

Contractbeheer op het terrein van IT niet op orde

Door de strikte scheiding van inkoop, behoeftestelling en financiële controle is het bijzonder moeilijk geworden om belangen te vermengen of invloed uit te oefenen op aanbestedingen. Het is lastig om een persoonlijk of commercieel belang te dienen. Maar alle regels en lange werkprocessen hebben de rechtmatigheidsproblemen in het contractbeheer op het terrein van IT niet kunnen verhelpen.

Door het uitblijven van een centraal contractenregister, aanbevolen door de auditdienst, mist het ministerie van Defensie managementinformatie die signalen oplevert voor tijdige contractverlenging. Deze managementinformatie kan ook worden gebruikt om risicoanalyses te maken ten aanzien van belangenverstrengeling, afhankelijkheden van bepaalde bedrijven en langdurige inhuur van externe medewerkers.

Verwervingsprocedures duren te lang voor aanschaf IT

Bij IT-projecten knellen lange procedures nog meer dan bij andere aanbestedingen. De technische ontwikkelingen in de IT gaan snel waardoor een informatie-intensief ministerie als het ministerie van Defensie achter gaat lopen als met het inkoopproces niet snel en flexibel kan worden gereageerd op nieuwe behoeften en nieuwe productmogelijkheden. De BIT-procedure die sinds kort van kracht is naar aanleiding van de parlementaire enquête ICT is een extra stap in de procedure, die het proces mogelijk nog verder doet uitlopen.

4.2 Tweede thema: de relatie Defensie - markt

Gemakkelijke toegang acounthouders bedrijven roept vragen op bij defensiemedewerkers

Accountmanagers en ook andere vertegenwoordigers van IT-bedrijven hebben een goed netwerk binnen de defensieorganisatie. Zij kennen het ministerie vaak al vele jaren. Sommigen hadden tot voor kort een toegangspas met verregaande toegang tot defensieterreinen. Een leidinggevende stelt dat hij gesprekken met accounthouders erg nuttig vindt: "Ik zit hier nog maar kort. Hij [de accountmanager] kent de IT bij Defensie al heel lang. Hij weet veel meer dan ik. Ik ben blij dat hij mij signalen geeft als er iets fout dreigt te gaan."

In veel gesprekken die wij voerden kwam aan de orde dat contacten tussen deze vertegenwoordigers van het bedrijfsleven en de ambtelijke top, vragen oproepen in de defensieorganisatie. Accountmanagers van bedrijven komen binnen op alle niveaus. Medewerkers van het ministerie zijn zich niet altijd bewust van de impact die dergelijke gesprekken elders in de organisatie hebben. Bij die contacten moet bijvoorbeeld gedacht worden aan de algemene gesprekken, die veelal plaatsvinden op verzoek van de vertegenwoordiger van een bedrijf: "Zullen we weer eens even bijpraten?" Medewerkers weten dat deze contacten plaatsvinden en vragen zich af wat er wordt besproken en besloten. Overigens dient de Tweede Kamer zich ervan te vergewissen dat ook de contacten die zij hebben met vertegenwoordigers van het bedrijfsleven het inkoopproces onder druk kunnen zetten.

Ook komt het voor dat accounthouders van bedrijven, of hun vertegenwoordigers, bovenlangs druk uitoefenen op het verloop van IT-projecten of aanbestedingen. Accounthouders strooien graag met namen: "Ik sprak gisteren die en die nog". Zo ontstaat snel het beeld dat in 'hoge achterkamertjes' dealtjes worden gemaakt en de aanbesteding eigenlijk al een gelopen race is. Leidinggevenden op hun beurt laten zich wel eens positief uit over bepaalde bedrijven ("Het kan toch niet zo zijn dat dit bedrijf afvalt in de aanbesteding"). Dat roept onmiddellijk vragen op over hun relatie tot dat bedrijf. Zo is ons voorgehouden, dat aan een leidinggevende na het functioneel leeftijdsontslag (FLO) wellicht een commissariaat is beloofd. Van dergelijke afspraken is ons niets gebleken.

Contacten met oud-defensiemedewerkers in dienst van het bedrijfsleven zijn een bron van vermoedens van belangenverstrengeling

Een aantal defensiemedewerkers treedt na het FLO in dienst van een IT-bedrijf. In het oog springend zijn oud-generaals die hoge posities bekleden binnen bedrijven. Zij kennen de organisatie en de behoeften in de organisatie als geen ander. Via hun netwerk komen zij makkelijk op veel plaatsen. "Als je oude commandant belt om even bij te praten, dan is het moeilijk om nee te zeggen. Zo komen bedrijven wel makkelijk binnen bij ons." Zeker bij deze contacten ontstaat snel de schijn van beïnvloeding.

Noorwegen stelt strengere eisen aan bedrijven die meedoen aan aanbestedingen
Het ministerie van Defensie kent, evenals de overige ministeries, een verbod op de zogenaamde draaideurconstructie. Het ministerie van Defensie van **Noorwegen** kent zo'n bepaling ook en vraagt van bedrijven die meedingen in aanbestedingen een expliciete verklaring over oud-defensiepersoneel:
"Former employees in the Defence Sector
Unless being out of the Defence Sector for more than two years, personnel in the Defence Sector should be cautious about having contact with former employees in procurement related matters. A company has to present a declaration together with a bid informing about former defence employees. This includes also retired personell. The aim is to avoid possible conflict of interest by increased transparency."

Contacten zijn soms te vriendschappelijk, waarbij teveel informatie wordt gedeeld

Bedrijven gebruiken hun netwerk binnen het ministerie van Defensie om informeel af te tasten waar marktkansen liggen en om toegang te krijgen tot het hogere management. Een belangrijke bevinding op dit vlak is dat volgens een bij de screening van bedrijven betrokken medewerker geen enkel Nederlands IT-bedrijf er dusdanige praktijken op nahoudt dat het op een zwarte lijst geplaatst zou moeten worden.

Dat neemt niet weg dat wij enkele voorbeelden hebben gehoord en gelezen van contacten die de grenzen van zakelijk verkeer overschrijden. "Hij mag me ook gewoon in het weekend bellen hoor. Ik heb lekkere wijnen." Soms wordt interne informatie doorgespeeld die duidelijk intern had moeten blijven. Ook de betrokken medewerkers zijn zich daar van bewust, getuige de toevoeging "Je hebt deze mail niet gehad" die wij her en der aantroffen. Ook is het voorgekomen dat informatie uit biedingen van bedrijven bekend werd bij een concurrent.

Bezoeken aan beurzen en studiereizen waren voorheen aanleiding tot vermoedens van belangenverstrengeling

Tot enkele jaren geleden kregen defensiemedewerkers wel uitnodigingen van bedrijven om mee te gaan naar een voetbalwedstrijd, om een *golfclinic* te doen, om een buitenlandse beurs te bezoeken of een studiereis te maken, etc. Dergelijke uitnodigingen zijn momenteel nauwelijks meer aan de orde. Bedrijven weten dat ambtenaren dergelijke cadeaus niet mogen aannemen en bieden deze niet meer aan. Wij hebben geen aanwijzingen gevonden dat er onregelmatigheden hebben plaatsgevonden rond (studie)reizen, in de zin dat reizen werden aangeboden in ruil voor directe tegenprestaties.

Voor de accountantsdienst is er nooit aanleiding geweest om nader onderzoek te doen naar uitgaven aan reizen. Wel kan geconstateerd worden dat dergelijke studiereizen of het bezoeken van buitenlandse beurzen, aanleiding zijn geweest tot vermoedens van belangenverstrengeling. Het kwam voor dat verschillende mensen van één afdeling samen naar een congres of beurs in bijvoorbeeld Las Vegas gingen. Dat heeft dan meer het karakter van een personeelsuitje dan van een zakelijke reis.

Nevenfuncties verrichten zonder goede afspraken levert integriteitsrisico's op
Sommige medewerkers hebben een eigen bedrijf naast hun werk voor het ministerie van Defensie. Dat is toegestaan, mits er goede afspraken worden gemaakt. Het aanmelden van nevenwerkzaamheden is daarvoor de start, dat schrijft de interne regelgeving ook voor. Wij constateren uit de gevoerde gesprekken dat niet elke leidinggevende strakke afspraken maakt met zijn of haar medewerkers over wat er wel of niet mag als nevenwerkzaamheden. Zo spraken wij een medewerker die als zzp-er advieswerk doet op het terrein waarin hij ook voor het ministerie werkzaam is, zonder heldere afspraken op papier te hebben welke klanten hij wel en niet mag bedienen.

Reservisten: integriteit is 'dode hoek' in het beleid
Eén van de aanleidingen voor ons onderzoek was de casus over de reservist die vanuit Afghanistan mailde met zijn moederbedrijf. Televisieprogramma Zembla berichtte hierover in september 2014. Onze bevinding uit vele gesprekken over de inzet van reservisten is dat er een zogenaamde 'dode hoek' zit in het reservistenbeleid. Desgevraagd blijkt er geen standaardprocedure te zijn voor de afweging of op een positie een reservist kan worden ingezet of niet. Sommige leidinggevenden hanteren een eigen afwegingskader, anderen geven aan dat inzet op alle plekken mogelijk zou moeten zijn omdat reservisten gescreend worden[10].

We zien in veel gesprekken dat inzet van reservisten op functies waar gewerkt wordt met zeer gevoelige informatie vragen oproept over de veiligheid en over het voorkomen van (de schijn van) belangenverstrengeling.

Het is niet goed uit te leggen dat reservisten tijdens hun passieve militaire status een geactiveerde defensiepas op zak hebben en daarmee vele -soms ook vitale- terreinen van het ministerie kunnen betreden. Reservisten worden beschouwd als interne defensiemedewerkers en hebben een zogenaamde type-1 pas.

Onderwerpen uit het thema 'relatie Defensie – markt' zijn internationaal moeilijk vergelijkbaar

Internationale vergelijkingen, op zoek naar te leren lessen, zijn lastig bij de onderwerpen die in deze paragraaf aan de orde komen. In veel landen, zoals het **Verenigd Koninkrijk** en de **Verenigde Staten**, is de verwevenheid tussen bedrijfsleven en de krijgsmacht groter dan in Nederland. Personeel stapt, in beide landen, vaker over van de krijgsmacht naar het bedrijfsleven en vice versa. Niet alleen aan het eind van een loopbaan maar ook als reguliere carrièrestap. Een medewerker van een defensieafdeling van een Nederlandse ambassade had op het terrein van verwerving een contactpersoon van het ministerie van Defensie. Die nam ontslag en enkele weken later zat de contactpersoon aan dezelfde overlegtafel, namens een groot bedrijf.
Er zijn in de Verenigde Staten en het Verenigd Koninkrijk (al) veel meer reservisten dan momenteel in Nederland en die staan maatschappelijk hoog in aanzien. Vragen over integriteit zijn er niet of nauwelijks. De conclusie dat je niet twee heren kunt dienen, vindt in de Verenigde Staten geen weerklank. Als reservist dien je immers je land.

[10] Er bestaat wel een document van COID over reservisten en nevenwerkzaamheden. Met dat laatste wordt bedoeld de hoofdfunctie van betrokkene, buiten Defensie. Dit stuk wordt echter niet Defensiebreed gebruikt. Het stuk geeft richtlijnen hoe risico's kunnen worden ingeschat ten aanzien van de civiele hoofdtaak van reservisten. Helaas komt de prealabele vraag niet aan de orde óf op de betreffende functie een reservist kan worden geplaatst.

Gedrag reservisten is aanleiding voor vermoedens van belangenverstrengeling

Een zaak die wij in extenso hebben onderzocht, is een melding over een aantal reservisten dat een IT-applicatie had gebouwd voor gebruik in een uitzendgebied. Bij het voorbereiden van een nieuwe uitzending in een ander land, kregen defensiemedewerkers het gevoel dat deze applicatie door de reservisten werd gepromoot. Er rezen vragen over hun gedrag: hadden de reservisten of hun moederbedrijven voordeel bij een grootschaliger gebruik van de applicatie?

Uit ons onderzoek blijkt dat er afspraken waren tussen betrokken reservisten en het ministerie van Defensie over eigendom en gebruik. Het promoten van de applicatie voor andere uitzendingen gebeurde in opdracht van enkele betrokken commandanten die een grootschaliger gebruik van de applicatie om operationele doeleinden verstandig vonden.

Eén van de commandanten sprak één van de reservisten overigens wel aan op het feit dat deze zijn bedrijfsnaam gebruikte op presentaties. De commandant wees hem er op dat hij zo de schijn van belangenverstrengeling wekte. Op basis van onze reconstructie constateren we dat er geen sprake was van belangenverstrengeling, maar wij kunnen goed begrijpen dat de vermoedens van belangenverstrengeling wel zijn gerezen.

Defensiepassen

In gesprekken over verstrekking van defensiepassen is ons steeds meegedeeld dat naast de fysieke beveiliging van defensieterreinen ook andere vormen van beveiliging van belang zijn. Wij zijn van mening dat de defensiepas toch grote mogelijkheden biedt om gemakkelijk op militaire terreinen te komen. Een defensiepas wordt gebruikt als middel voor identificatie, authenticatie en autorisatie. Uit een inventarisatie blijkt dat er externen zonder een directe arbeidsrelatie zijn, die beschikken over een defensiepas, soms meerdere jaren geldig. Wij constateren uit de inventarisatie ook dat het beheer van passen die aan leveranciers ter beschikking worden gesteld te wensen overlaat. Daaronder valt ook het toezien op inname van verlopen defensiepassen. Een deel van de verlopen passen blijkt niet te zijn ingenomen.

Conclusies over de relatie Defensie – markt:

Toegang van het bedrijfsleven tot medewerkers van Defensie is te gemakkelijk

Accountmanagers en andere vertegenwoordigers van bedrijven komen te gemakkelijk binnen bij medewerkers van het ministerie. Medewerkers zijn zich onvoldoende bewust van het feit dat dergelijke gesprekken elders in de organisatie snel de schijn van beïnvloeding wekken.

Te vriendschappelijke contacten

Defensiemedewerkers en vertegenwoordigers werken soms lang samen. Dan ontstaan soms te vriendschappelijke relaties. In die situaties wordt het defensiebelang niet meer goed onderscheiden van het commerciële belang van het bedrijf en wordt informatie uitgewisseld die op het ministerie had moeten blijven.

'Dode hoek' in het reservistenbeleid

Er zit een zogenaamde 'dode hoek' in het reservistenbeleid. Bij het bepalen of een reservist kan worden ingezet op een functie en zo ja welke, wordt te weinig rekening gehouden met het feit dat een reservist per definitie twee heren dient. Een reservist heeft zijn of haar eigen broodheer en dient daarnaast ook het ministerie van Defensie. Of andersom. Dat hoeft niet per se te knellen. Maar bij reservisten die worden ingezet om hun specifieke IT-deskundigheid, kan dat wel het geval zijn: zij krijgen inzicht in behoeften van het ministerie van Defensie die anderen niet hebben. Dat geldt voor medewerkers van (IT-)bedrijven, maar ook voor zzp-ers. Zij hebben er belang bij steeds nieuwe opdrachten te doen voor het ministerie van Defensie. De vraag of dat erg is, en zo ja welke mitigerende maatregelen genomen moeten worden, is geen standaard onderdeel van het reservistenbeleid.

4.3 Derde thema: melden en het behandelen van meldingen

Informatieachterstand leidt tot vermoedens van belangenverstrengeling

In elke organisatie spelen integriteitszaken. Vermoedens van belangenverstrengeling komen overal voor. Soms door daadwerkelijke verstrengeling van belangen. In ons onderzoek zien we dat vermoedens van belangenverstrengeling in een flink aantal gevallen ook ontstaan, doordat medewerkers een informatieachterstand hebben. Dit speelde onder meer een rol bij het *sourcings*vraagstuk en de vermoedens over torenhoge bindingspremies.

Een ander voorbeeld is de implementatie van een technische voorziening in een uitzendgebied. Door vertraging in de uitvoering ontstonden ter plekke problemen. Op verzoek van de commandant deed een aantal defensiemedewerkers onderzoek of ter plekke een oplossing kon worden gevonden met bedrijven in een stad in het uitzendgebied. Dat leek te kunnen en zou vele malen goedkoper zijn dan de reguliere oplossing via Nederland. Echter, op dat moment werd er toch opeens een Nederlands bedrijf ingezet om de voorziening te leveren. Medewerkers begrepen dat niet en vermoedden belangenverstrengeling.

Uit ons onderzoek blijkt dat de onderzochte oplossing met buitenlandse bedrijven niet paste binnen de defensiebrede regels voor informatiebeveiliging en bovendien voorbij ging aan bestaande (raam)contracten. Als over deze contracten en de regels omtrent de levering van de voorziening helder was gecommuniceerd naar het uitzendgebied, dan had men zich de energie kunnen besparen om lokale oplossingen te zoeken en waren de vermoedens van belangenverstrengeling niet ontstaan. En uiteraard had de voorziening ook veel sneller geleverd moeten worden.

Veel plekken voor meldingen en vragen, maar medewerkers weten niet waar zij het best heen kunnen

Defensiemedewerkers die vermoedens hebben van misstanden in de omgang tussen het ministerie en commerciële partijen op het terrein van de IT kunnen op veel plekken terecht voor informatie of voor het doen van een melding. De voorgeschreven weg is een melding aan de direct leidinggevende, mondeling of via het digitale systeem Melden van Voorvallen (MVV). Als melden bij de leidinggevende niet kan, is het alternatief een melding bij het meldpunt van de Centrale Organisatie Integriteit Defensie (COID), en als dat ook niet kan bij een extern meldpunt (bijvoorbeeld de Ombudsman).

Echter, uit onze gesprekken blijkt dat lang niet iedereen het meldpunt van COID kent. Het MVV-systeem is, zo hebben wij ook zelf proefondervindelijk geconstateerd, weinig gebruiksvriendelijk. Het systeem wordt als onveilig ervaren omdat een melding – na actie van de leidinggevende – aan een grote groep medewerkers wordt verzonden. Bovendien is niet duidelijk wie er actie moet ondernemen. Niet-opvolgen van meldingen leidt niet tot signalering[11].

En er zijn er nog veel meer plekken waar medewerkers terecht kunnen met hun vragen en vermoedens: de vertrouwenspersonen integriteit, de inspecteur-generaal der Krijgsmacht (IGK), geestelijk verzorgers, de MIVD, de Kmar, bedrijfsmaatschappelijk werk[12]. Een deel van deze mogelijkheden wordt beschreven in de interne regelgeving, andere mogelijkheden worden eigener beweging aangeboord door medewerkers die ergens mee rondlopen.

---

[11] Het afgelopen jaar is gewerkt aan verbeteringen in het MVV-systeem. Onze indruk is echter dat de voornaamste bezwaren in de toepasbaarheid van het systeem zullen blijven bestaan.

[12] Bijkomend probleem is dat de centrale registratie van meldingen te wensen over laat. Het is derhalve niet te zeggen hoeveel meldingen er jaarlijks binnenkomen over vermoedens van integriteitschendingen in de omgang tussen het ministerie en commerciële partijen op het terrein van de IT.

Wij constateren dat er geen standaardwerkwijze is hoe omgegaan moet worden met meldingen. Er zijn wel handreikingen waarin staat wat hij of zij dan kan doen, maar er wordt veel overgelaten aan de inschatting van de betrokken commandant.

Wij constateren bovendien dat veel medewerkers hun vragen ook niet zozeer zien in het licht van een mogelijke integriteitschending. Hun zorgen komen voort uit een groot inhoudelijk verantwoordelijkheidsgevoel voor de veiligheid van de IT-systemen en cruciale netwerken. Enkele malen vroeg men ons letterlijk: "Oh, is dat dan ook integriteit?"

Defensiemedewerkers die na het stellen van een vraag of het doen van een melding krijgen soms vermoedens dat er een doofpot is

Een veel gehoorde klacht is, dat men na het doen van een mondelinge of digitale melding niets meer hoort. Dat roept bij medewerkers soms het vermoeden op dat 'de leiding' dan wel wat te verbergen zal hebben. Vertrouwenspersonen genieten niet altijd voldoende vertrouwen, zo blijkt uit gesprekken.

Wij willen hier in het bijzonder wijzen op meldingen bij de MIVD. Sommige melders wenden zich tot de MIVD omdat zij vermoeden dat de staatsveiligheid in het geding is. De verwachting is vervolgens dat de MIVD zal optreden om het (vermeende) probleem op te lossen. De MIVD gebruikt informatie echter veelal voor andere doeleinden en kan melders ook niet informeren over de werkwijze en eventueel genomen stappen. Het kan ook zijn dat een MIVD-medewerker besluit niets met de informatie te doen, bijvoorbeeld omdat de inschatting is dat de staatsveiligheid niet in het geding is en het daarom geen zaak voor de MIVD is. Melders horen niks meer, raken teleurgesteld of krijgen vermoedens dat zaken in de doofpot worden gestopt.

Kritische vragen van defensiemedewerkers worden niet beantwoord

Defensiemedewerkers vertelden ons zaken waarvan ze niet zeker wisten of het een misstand was, maar die hen in elk geval niet lekker zaten. Het ging daarbij over operationele vraagstukken (is onze database wel bijgewerkt; is deze IT-toepassing wel veilig; waarom worden noodprocedures niet geoefend; er zijn te weinig mensen om de boel draaiend te houden; we krijgen te weinig opleiding), over veranderingen in het werk (wel of niet *sourcen*; een verhuizing; een nieuw rooster, reorganisaties; steeds wisselende managers) en over slecht lopende IT-projecten en externe inhuur (waarom kiest u deze projectleider; waarom krijgen externen zoveel betaald; waarom wordt er steeds een IT-oplossing doorgedrukt terwijl wij als gebruikers er niet mee uit de voeten kunnen).

De vragen die medewerkers bij ons op tafel legden hadden zij veelal ook gesteld aan hun leidinggevenden. Maar ze kregen – zo gaven zij aan – geen duidelijk antwoord. Veel gesprekspartners denken bovendien dat het hogere management door het middenmanagement niet goed wordt geïnformeerd over zaken die spelen op de werkvloer. Het resultaat van deze gang van zaken is dat medewerkers zich niet serieus genomen voelen en niet meer bereid zijn om zaken te melden die mogelijk niet door de beugel kunnen. Ook zoeken medewerkers zelf verklaringen voor vragen waar zij mee zitten.

COID wordt internationaal als voorbeeld gezien

Wij hebben geen informatie gekregen dat ministeries van Defensie in andere landen een aparte integriteitsorganisatie hebben vergelijkbaar met de COID. Nog sterker, COID en defensieafdelingen van Nederlandse ambassades krijgen vragen van andere landen omdat die COID als voorbeeld zien. Ook andere initiatieven van het Nederlandse ministerie van Defensie staan internationaal in de belangstelling, zoals de dilemmakaarten die de Kmar gebruikt. Die kaarten zijn inmiddels ook in het Engels beschikbaar.

Conclusies over melden en het behandelen van meldingen:

Veilig melden van misstanden is moeilijk, zo niet onmogelijk

Ondanks de overdaad aan plekken waar men vragen kan stellen en kan melden, weten veel defensiemedewerkers die ergens mee rondlopen niet waar ze hun verhaal kwijt kunnen. Het is onduidelijk – op papier maar zeker in de praktijk – wat er moet gebeuren met meldingen die op andere plekken worden gedaan dan bij de leidinggevende of het COID. Ook komt het voor dat een medewerker in de veronderstelling is dat hij of zij een melding heeft gedaan, terwijl de ontvanger de eigen rol anders ziet, bijvoorbeeld als adviseur. Meldingen kunnen makkelijk tussen wal en schip komen. Vertrouwenspersonen en het MVV genieten niet altijd voldoende vertrouwen. Het meldpunt van COID is niet bij iedereen bekend.

Geen eenduidige behandeling van meldingen

Een eenduidige behandeling van meldingen ontbreekt. Daardoor weten melders ook niet wat zij kunnen verwachten. De afhandeling van meldingen duurt vaak erg lang of afronding vindt niet plaats. Melders horen soms niets meer terug. Onderdelen hebben allemaal hun eigen behandelwijze, al dan niet op papier. Soms beslissen individuele medewerkers, bijvoorbeeld bij de MIVD, om een vraag of melding niet op te volgen en daarover niet te communiceren.

Het adagium 'de commandant is er van' is begrijpelijk. Bevordering van integriteit en het behandelen van vermoedens van integriteitschendingen is een belangrijke taak van de direct leidinggevende. Dat neemt niet weg dat de commandant vlot op moet schalen bij complexe situaties.

COID is niet goed gepositioneerd en mist enkele functies

De ophanging als Bijzondere Organisatie Eenheid onder het Commando Diensten Centrum (CDC) is – ook voor de beeldvorming – te ver van de SG weggeorganiseerd. COID mist momenteel enkele functies: een klokkenluidersloket ontbreekt en ook de *compliance* functie is onvoldoende ingericht. Inrichting van een regelgeving voor financiële *compliance* loopt achter bij de toezeggingen. COID stelt zich op als adviseur, maar zou ook aanjager en procesbegeleider moeten zijn. In de praktijk is er veel discussie over 'wie doet wat' tussen Hoofddirectie Personeel (beleid en toezicht), COID, juridische onderdelen, de lokale vertrouwenspersonen en de coördinatoren vertrouwenspersonen die bij elk operationeel commando werkzaam zijn.

5 Hoofdconclusie en beantwoording van de deelvragen

5.1 Hoofdconclusie

De hoofdvraag van dit onderzoek was:

Brengt de manier waarop door het ministerie van Defensie wordt omgegaan met commerciële partijen op het gebied van IT de integriteit van de defensieorganisatie in het geding?

Ons antwoord op deze hoofdvraag, onze hoofdconclusie, is tweeledig.

Ten eerste. De commissie heeft, op één geval na, geen aanleiding gevonden om specifieke feiten of gedragingen van personen, die strijdig zouden zijn met wet- en regelgeving, onder de aandacht van de secretaris-generaal te brengen. Wij hebben in de gesprekken en in de bestudeerde documenten geen inbreuken op de integriteit kunnen vaststellen in de zin van corruptie, omkoping, fraude, daadwerkelijke belangenverstrengeling of het te eigen bate misbruiken of manipuleren van informatie. Dat geldt voor de zaken die de directe aanleiding vormden voor ons onderzoek, maar ook voor de andere onderzochte casuïstiek. Defensiemedewerkers handelden in het verleden niet altijd conform de regelgeving bij het contracteren van tijdelijke externe medewerkers voor IT-projecten. Deze onregelmatigheden werden in de controlelijn aan de orde gesteld. De reactie daarop was veelal dat er druk op betrokkenen werd uitgeoefend. Wij hebben geen nieuwe onrechtmatigheden geconstateerd. Er doen zich echter nog steeds risico's voor op het gebied van het contractbeheer bij IT-projecten. Contracten dreigen te verlopen terwijl dienstverlening doorgaat. De vormgeving van het aanbestedingsproces is hier mede debet aan. Op dit punt is de integriteit van de defensieorganisatie in het geding: het inhuren van mensen of diensten op basis van een niet-adequaat vastgesteld contract is onrechtmatig en raakt dus de integriteit van deze inhuur.

Ten tweede. Het feit dat wij geen daadwerkelijke integriteitschendingen vaststellen brengt ons niet tot de conclusie dat er niks aan de hand is of dat het 'wel mee valt'. In hoofdstuk één en drie betoogden wij dat integriteitsvragen niet kunnen worden onderzocht aan de hand van louter juridische vragen. Integriteit dient breder te worden beschouwd en kent ook een ethische en een bestuurlijke dimensie. In dat licht bezien is er actie nodig, omdat op het terrein van IT in de afgelopen jaren op diverse plekken in de organisatie de schijn van belangenverstrengeling is gewekt. De aanleiding verschilt: opeenvolgende reorganisaties, trage en rommelige procesgang bij aanbestedingen of IT-projecten, het toelaten van accountmanagers van bedrijven, onduidelijkheden over de inzet van reservisten, het steeds inhuren van dezelfde externe medewerker, etc. Deze zaken vormen een vruchtbare voedingsbodem voor het ontstaan van vermoedens van belangenverstrengeling en moeten worden aangepakt. Belangrijk daarbij is, om de onderliggende oorzaken weg te nemen voor het ontstaan én voortbestaan van vermoedens van belangenverstrengeling: onduidelijke communicatie, het niet beantwoorden van vragen van medewerkers, en het niet adequaat behandelen van meldingen. Zonder actie op deze punten is de integriteit van de defensieorganisatie in het geding.

5.2 Beantwoording van de deelvragen

Is er door medewerkers van het ministerie van Defensie of door medewerkers die (extern) door Defensie zijn ingehuurd in de omgang met commerciële partijen op het gebied van IV en ICT gehandeld in strijd met wet- en (interne) regelgeving?

In het verleden is door medewerkers van het ministerie van Defensie en door extern ingehuurde medewerkers in enkele gevallen gehandeld in strijd met regelgeving op het vlak van aanbestedingen. Onregelmatigheden betroffen vooral het te laat verlengen van contracten en het zeer lang inhuren van bepaalde externe medewerkers. In het contractbeheer doen zich nog altijd risico's voor die moeten worden aangepakt. De commissie heeft, op één geval na, geen aanleiding gevonden om specifieke feiten of gedragingen van personen, die strijdig zouden zijn met wet- en regelgeving, onder de aandacht van de secretaris-generaal te brengen. Wij hebben in de gesprekken en in de bestudeerde documenten geen inbreuken op de integriteit kunnen vaststellen in de zin van corruptie, omkoping, fraude, daadwerkelijke belangenverstrengeling of het te eigen bate misbruiken of manipuleren van informatie.

In hoeverre kan er voordeel zijn voor medewerkers en/of commerciële partijen bij een dergelijke handelswijze?

Wij hebben geen gevallen aangetroffen waar defensiemedewerkers persoonlijk voordeel ontleenden aan de omgang met commerciële partijen op het gebied van de IT. Wel troffen wij situaties aan waarin afspraken over het vervullen van nevenfuncties niet voldoende waren vastgelegd.

Commerciële partijen zelf hebben soms voordeel gehad bij bovengenoemde handelwijze: medewerkers konden zeer lang worden ingezet bij het ministerie. In één geval kreeg een externe projectleider zoveel mandaat dat hij een bepalende rol had bij het aannemen van andere externe medewerkers.

Wat zijn de achterliggende oorzaken van de omgangswijze?

De hierboven beschreven zaken konden ontstaan in een complexe situatie met forse bezuinigingen, achtereenvolgende reorganisaties, grote, langdurige projecten waar veel tijdsdruk op stond, een onvoldoende ingericht contractbeheer en een moeizaam functionerende bureaucratie met versnipperde verantwoordelijkheden. Bovendien is de doorlooptijd van sommige projecten langer dan de aanstellingsduur van een projectverantwoordelijke. Denk aan de projectleider van een grote aanbesteding of de projectleider van een omvangrijk IT-project. Wanneer er dan geen goede overdracht plaatsvindt, kan door anderen – zoals commerciële partijen - gebruik gemaakt worden van de gelegenheid om er meer uit te halen dan is toegestaan.

Is er sprake van een praktijk waarbij binnen het IT-domein nauwe banden met commerciële partijen ontstaan?

Nauwe banden zijn er, en die zijn ook noodzakelijk. Het ministerie van Defensie kon de afgelopen jaren niet zonder externe deskundigheid op het gebied van IT en dat zal in de toekomst niet veranderen. Integendeel. De afhankelijkheid van innovaties in de markt zal alleen maar toenemen. Productinnovaties worden in de regel aangeboord in de industrie en niet binnen ministeries. Het ministerie is zich bewust van de noodzaak om - gegeven de nauwe banden - rollen en verantwoordelijkheden goed af te bakenen, functies te scheiden en een *level playing field* te creëren bij aanbestedingen. De interne regelgeving op dit vlak is in orde.

Wij hebben echter een aantal voorbeelden gezien van te warme contacten. Soms ontstaat een relatie waarbij informatie wordt uitgewisseld die op het ministerie moet blijven, zoals informatie uit biedingen van andere partijen en informatie over interne beraadslagingen over strategische technologische keuzes.

Reservisten verkeren in een positie dat zij twee heren dienen. Zij worden door hun beide werkgevers per definitie in een lastige situatie gebracht. Er is onvoldoende aandacht voor die spagaat.

In hoeverre worden daarbij ongewenste beïnvloedingsstrategieën gehanteerd door commerciële partijen in de IT sector?

Vertegenwoordigers van het bedrijfsleven hebben vaak een zeer langdurige relatie met het ministerie. Zij hebben er soms zelf gewerkt. Zij kennen veel mensen en ook de behoeften van de organisatie. Het is niet meer dan logisch dat zij beïnvloedingsstrategieën hanteren: gesprekken met werknemers en leiding, organiseren van seminars en symposia, deelname aan beurzen etc. Wij constateren dat zaken als (groepsgewijze) deelname aan studiereizen, beurzen en symposia en het ruimhartig toestemmen in gespreksverzoeken door vertegenwoordigers van bedrijven soms vermoedens oproepen dat besluitvorming over aanschaffingen wordt beïnvloed.

6 Aanbevelingen

6.1 Hoofdaanbeveling: blijf oefenen om moreel fit te zijn en te blijven

Zoals wij in het eerste hoofdstuk hebben aangegeven, is onze belangrijkste aanbeveling dat het ministerie van Defensie intensief moet oefenen om moreel fit te zijn en te blijven. Er staan veel zaken op papier en in opleidingen is er aandacht voor integriteit. Maar het bevorderen van moreel aanvaardbaar gedrag vergt continue aandacht. Net als bij gewone fitness geldt: een paar dagen niet geoefend betekent minder lenigheid, minder kracht.

Moral fitness vraagt om een brede blik op integriteit. Een blik die integriteitszaken, vermoedens van integriteitschendingen en andere meldingen niet reduceert tot een juridische afvink-exercitie. Een blik die rekening houdt met bestuurlijke en ethische aspecten van integriteit. *Moral fitness* vraagt om het besef bij alle defensiemedewerkers dat 'integriteit' niet iets zwaars is, maar juist een alledaags begrip dat vraagt om heldere communicatie en het adequaat reageren op vragen en zorgen.

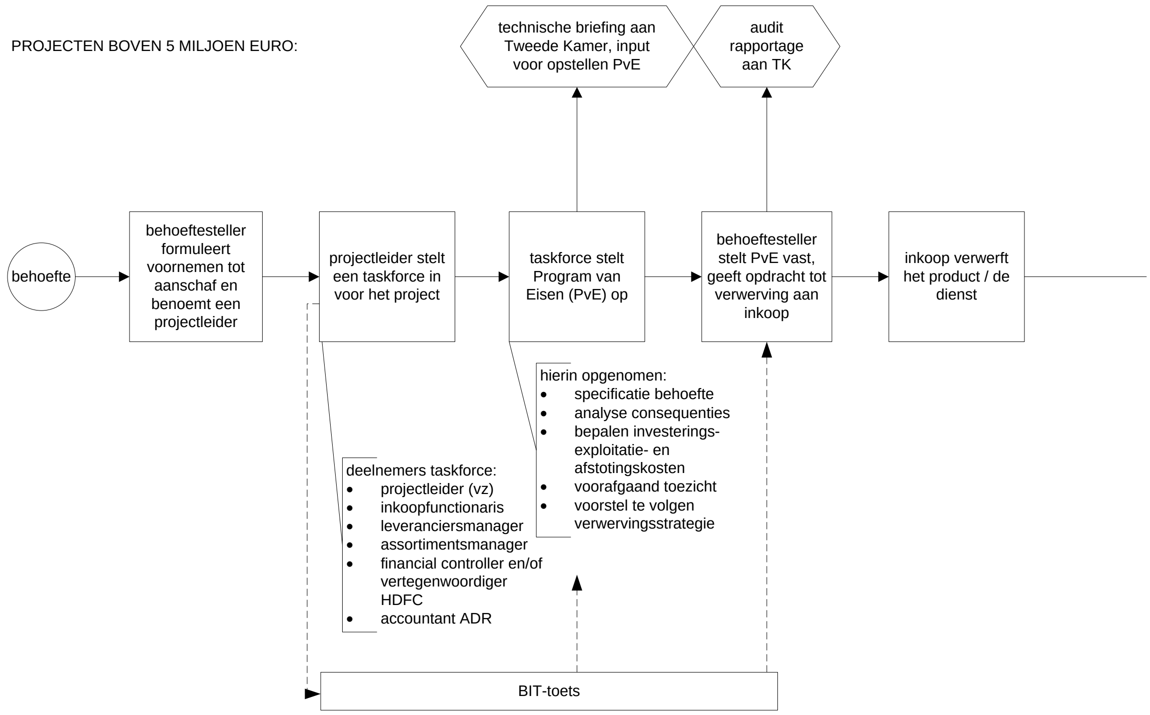
In de volgende paragrafen doen wij enkele aanbevelingen voor de drie dominante thema's die wij in hoofdstuk vier introduceerden. Deze zaken zijn nodig om moreel fit te worden en te blijven.

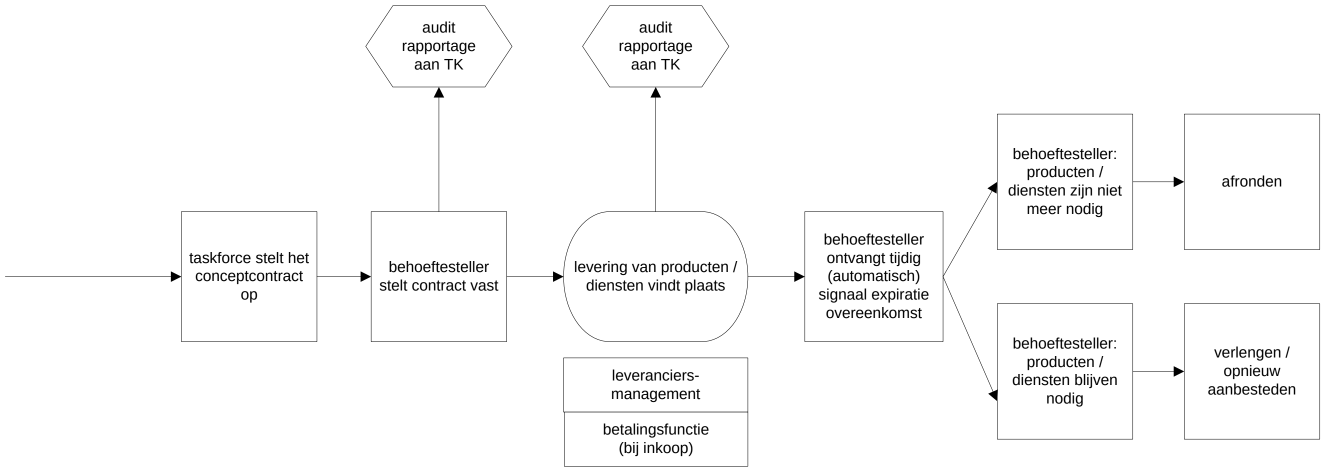
> Het kan raadzaam zijn om iemand te benoemen die de voortgang van de uitvoering van de aanbevelingen kritisch beoordeelt. Iemand die het proces volgt en direct concrete aanbevelingen geeft als zaken beter moeten of sneller kunnen. Zo'n procesbewaker past beter bij het type aanbevelingen dat wij doen dan een ex-post evaluatieonderzoek dat na jaren weer een volgend rapport oplevert. Vragen voor de procesbewaker zijn onder meer:
> - Worden de aanbevelingen uitgevoerd?
> - Wordt daarover voldoende gecommuniceerd?
> - Worden opkomende vragen afdoende beantwoord?
> - Treden de verwachte effecten op?
> - Zo nee, welke aanpassingen zijn nodig?

6.2 Verwerven en contractbeheer: versnel de aanbestedingen voor de verwerving van IT en zorg voor beter contractbeheer

- Wij bevelen aan om de aanbesteding van IT-producten en –diensten te versnellen. Daartoe bevelen wij aan om voor elke aanbesteding een projectteam samen te stellen waarin alle betrokken onderdelen vanaf dag één samenwerken. Het projectteam lijkt op de zogenaamde 'groene stip' die soms al wordt gebruikt bij aanbestedingen van het ministerie. Met zo'n aanpak kan naar schatting driekwart van de stappen in het huidige proces worden geschrapt of worden samengevoegd. Te denken valt aan het stappenplan dat op de volgende pagina wordt gepresenteerd. Het is gebaseerd op het aanbestedingsproces zoals dat nu wordt gebruikt bij het ministerie van Defensie. De behoeftesteller is in de *lead*. De door de behoeftesteller benoemde projectleider is verantwoordelijk voor het gehele proces inclusief de doorlooptijd. Ook de BIT-onderzoekers zouden in een dergelijke aanpak zo vroeg mogelijk in het proces deel kunnen nemen.

Stroomschema: verwerven van IT-diensten




taskforce stelt het conceptcontract op
behoeftesteller stelt contract vast
audit rapportage aan TK
levering van producten / diensten vindt plaats
audit rapportage aan TK
leveranciers-management
betalingsfunctie (bij inkoop)
behoeftesteller ontvangt tijdig (automatisch) signaal expiratie overeenkomst
behoeftesteller: producten / diensten zijn niet meer nodig
afronden
behoeftesteller: producten / diensten blijven nodig
verlengen / opnieuw aanbesteden

- Dit stroomschema hebben wij ontwikkeld als hulpmiddel om de aanbestedingsprocedure te versnellen. Het toepassen van het gesuggereerde stroomschema vergt veel van het ministerie. Het zal naar het gevoel van betrokken medewerkers indruisen tegen de scheiding van rollen die in de afgelopen jaren is aangebracht. In ons schema blijven rollen echter gescheiden, maar wordt wel vanaf het begin tot het eind samengewerkt. Bij problemen dient er vlot te worden geëscaleerd. Dat is geen teken van zwakte maar juist van goed projectmanagement. Leidinggevenden zijn verantwoordelijk voor het oppikken, opvolgen én tot oplossing brengen van signalen uit het team.

- Wij raden aan om een nieuwe, snellere aanpak eerst te testen in één of twee experimenten bij nieuwe aanbestedingen. Het is aan te bevelen om die experimenten te laten begeleiden door een (externe) procesbegeleider. Onderzocht kan worden of ook de Tweede Kamer deel uit wil maken van een dergelijke experimentele aanpak, want de procedure die met de volksvertegenwoordiging is afgesproken vraagt onnodig veel tijd. Mogelijk kan worden samengewerkt met Rijkswaterstaat waar momenteel ook experimenten plaatsvinden met anders en sneller aanbesteden[13]. Een meerjarig investeringsplan met een bestedingsparagraaf kan helpen om genomen investeringsbeslissingen vlotter uit te voeren[14].

- Wij bevelen aan om maatregelen te nemen om het contractbeheer te verbeteren. Van groot belang daarbij is het inrichten van een volledig digitaal contractenregister. Behoeftestellers dienen toegang te hebben tot dat register, en zij moeten tijdig een automatisch bericht ontvangen over aflopende contracten. Net als in het ontwikkelde stroomschema, bevelen wij aan dat de behoeftestellers – die kunnen op diverse plekken binnen het ministerie werkzaam zijn - verantwoordelijk worden voor het tijdig verlengen of opnieuw aanbesteden. Deze structuurverandering is naar onze mening nodig om de nu steeds dreigende onrechtmatigheden in het vervolg te vermijden.

6.3 De relatie Defensie – markt: stop met 'even bijpraten'-gesprekken met het bedrijfsleven en verwijder de 'dode hoek' uit het reservistenbeleid

- Wij bevelen aan om defensiebreed af te spreken dat medewerkers alleen spreken met vertegenwoordigers van het bedrijfsleven als dat een direct functioneel belang heeft. Denk aan inkopers die belast zijn met leveranciersmanagement. Om een 'ons kent ons' gevoel te voorkomen is het belangrijk dat inkopers regelmatig wisselen van functie of van portefeuille. Alle verzoeken van accounthouders of oud-officieren die een functie bekleden bij een bedrijf om 'even bij te praten' dienen te worden afgewezen. De ambtelijke top moet dit ook publiekelijk zeggen en blijven herhalen. Accounthouders en andere vertegenwoordigers van bedrijven behoren geen toegangspassen te hebben voor het ministerie. Dat geeft een verkeerd signaal. Het beheer van de uitgifte van passen en toezicht op de inname van verlopen passen kan beter.

- Uiteraard zal voorkomen dat wél met vertegenwoordigers van bedrijven moet worden gesproken. Het is niet nodig daar verkrampt over te doen. In die gevallen kan er voor gekozen worden om met een groep bedrijven tegelijk te spreken, of om het betreffende bedrijf wel te ontvangen en vervolgens breed te communiceren binnen het ministerie wat er besproken is. De ambtelijke top heeft hierin een voorbeeldfunctie.

---

[13] Zie http://www.magazinesrijkswaterstaat.nl/zakelijkeninnovatie/2015/02/minder-transactiekosten-bij-dbfm-contracten.

[14] Zie ook het recente rapport van Clingendael: *Multi-year Defence Agreements: a Model for Modern Defence?*

Het belang van de industrie om oud-medewerkers van het ministerie van Defensie aan zich te binden lijkt groter dan bij andere ministeries, onder meer omdat militairen de dienst via het FLO eerder verlaten dan rijksambtenaren. Bestudeer of het Noorse voorbeeld kan worden gevolgd om bij aanbestedingen transparantie te vragen over de inzet van oud-medewerkers. Bezie of nuttige expertise van defensiemedewerkers die met FLO gaan, kan worden behouden door de opzet van een adviesgroep waarin kennis van mensen kan worden verzilverd.

- Verder bevelen wij aan om de door ons beschreven 'dode hoek' in het reservistenbeleid aan te pakken. Bij functievervulling en opdrachtverlening aan reservisten moet allereerst de vraag aan de orde zijn of deze taak wel door een reservist kan worden vervuld. Het beantwoorden van die vraag kan leiden tot het nemen van maatregelen of het stellen van voorwaarden waaronder een reservist kan worden ingezet. Bij alle reservisten moet de vraag aan de orde zijn in hoeverre de hoofdfunctie van betrokkene belemmeringen oplevert voor de inzet. Dat kan leiden tot afspraken over de inzet en die horen op papier te staan. Het gesprek hierover is niet eenmalig maar moet regelmatig terugkeren (*moral fitness*). Dit geldt niet alleen voor reservisten die medewerker zijn van een (IT-)bedrijf, maar zeker ook voor reservisten die zzp-er zijn.

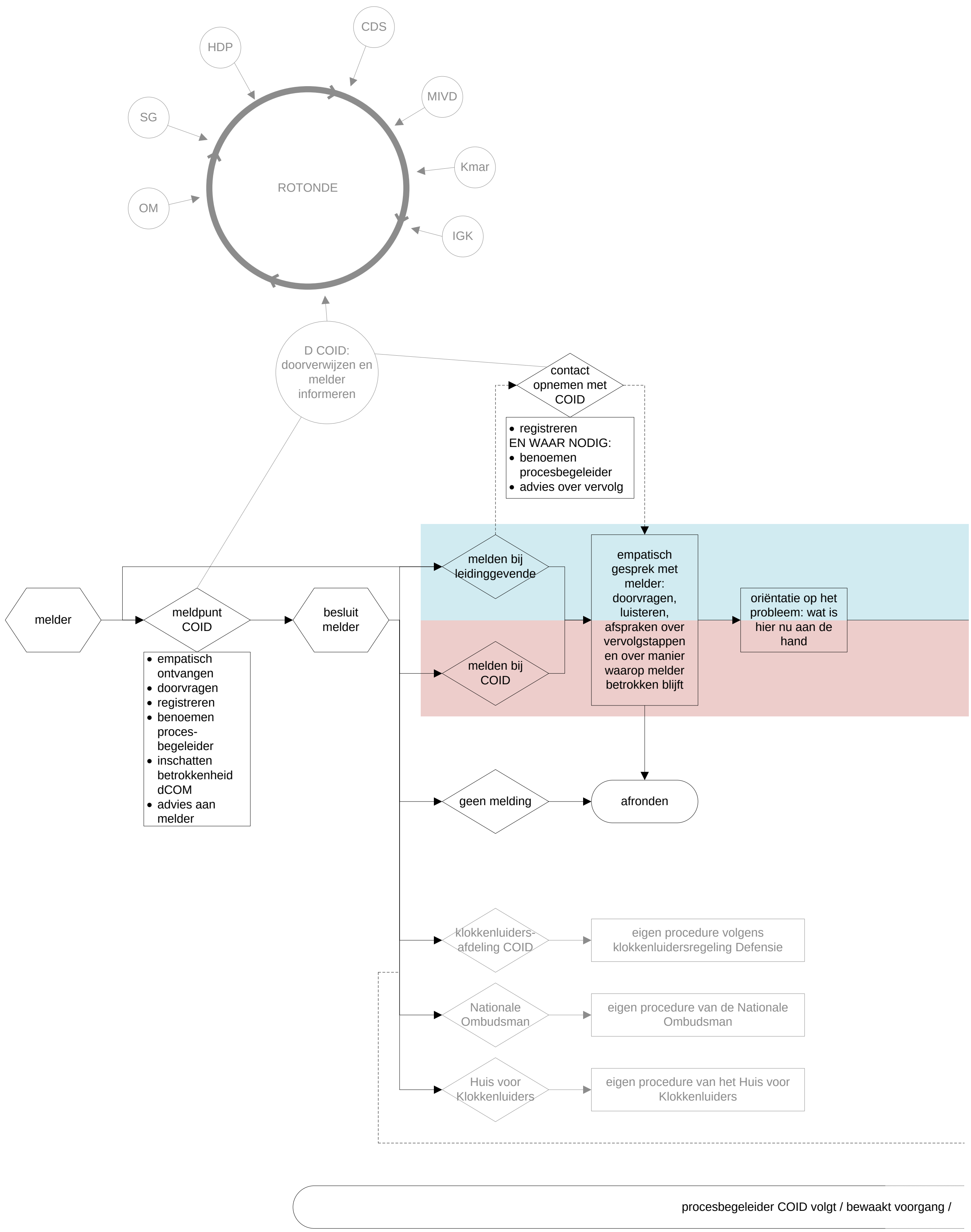
6.4 Melden en het behandelen van meldingen: behandel meldingen volgens één vaste lijn en geef COID daarin een steviger positie.

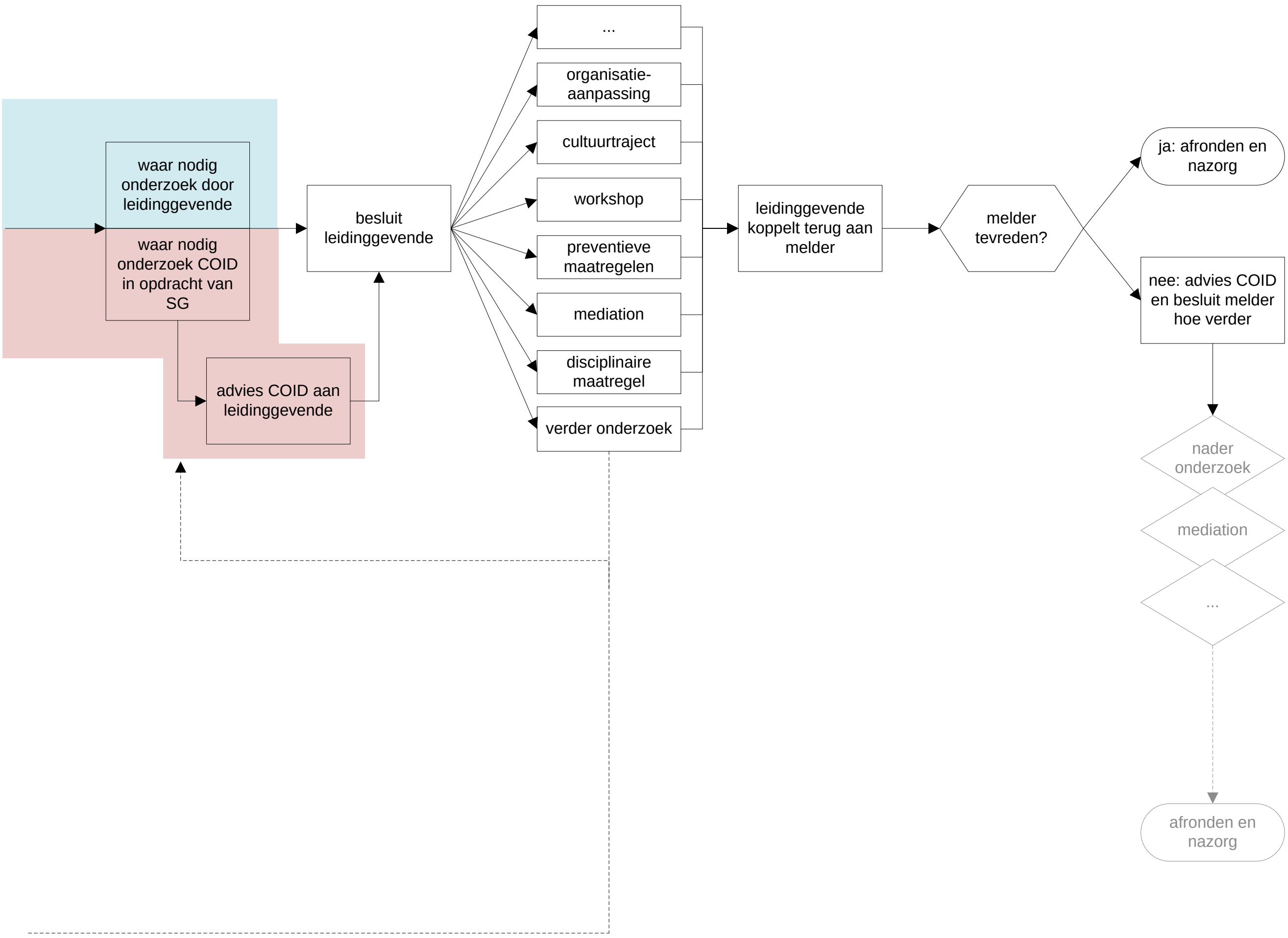
- Integriteit is *Chefsache*. Dat betekent dat de secretaris-generaal als hoogste ambtenaar dagelijks direct inzicht behoort te hebben in de integriteit van de defensieorganisatie. Wij bevelen aan om COID direct onder de SG te positioneren. Elke andere ophanging is *second best*. Een aantal taken op integriteitsgebied dat nu verspreid door het departement ligt, en taken die nog niet voldoende zijn opgepakt, kunnen worden samengebracht bij COID: integriteitsbeleid, de klokkenluidersregeling, de klachtencommissie ongewenste omgangsvormen, financiële *compliance* en de verantwoordelijkheid voor de taken en de kwaliteit van het netwerk van vertrouwenspersonen.

- Wij zeggen niet dat de huidige lijn dat commandanten verantwoordelijk zijn voor de integriteit van hun onderdeel moet worden losgelaten. Wel moeten meldingen worden behandeld volgens één vaste lijn en moeten complexe integriteitsvragen sneller worden 'opgekoppeld' naar een hoger ambtelijk niveau. Wij gebruiken de term 'opkoppelen' (van beneden naar boven melden) als het tegenovergestelde van terugkoppelen (van boven naar beneden melden). Wij bevelen aan om COID bij deze eenduidige behandeling een zwaardere rol te geven dan nu. Daarbij denken wij vooral aan triage en advisering over meldingen, aan procesbegeleiding bij de behandeling van meldingen en in voorkomende gevallen ook onderzoek naar meldingen. COID zou onzes inziens betrokken moeten zijn bij alle meldingen, ten behoeve van de eenduidige registratie.

- Wij hebben als suggestie voor verbetering van de meldprocedure een stroomschema ontwikkeld, waarin alle noodzakelijke stappen zijn opgenomen. Bij de gesuggereerde behandelingswijze komen meldingen binnen bij de commandant óf bij het meldpunt van COID. Als andere personen of onderdelen een melding ontvangen, verwijzen zij door naar één van deze twee mogelijkheden. Andere smaken zijn er niet. Het grote voordeel van een dergelijke behandelingswijze is dat de melder altijd op de hoogte is van de stand van zaken, dat een procesbegeleider mede let op een vlotte behandeling, en dat alle vragen en meldingen tot afronding komen. De spoedige ontwikkeling van een adequaat meldings- en registratiesysteem hoort bij de introductie van een eenduidige behandelingswijze.

Stroomschema: behandelen van meldingen





bewaakt betrokkenheid van en terugkoppeling aan melder / draagt zorg voor afronding en nazorg

- Wij bevelen aan dat meldingen die binnenkomen bij onderdelen als de MIVD, de Kmar, de IGK en ook het Openbaar Ministerie, waar relevant altijd op hoog niveau worden besproken. Daarbij kan het beeld in gedachten worden gehouden van een rotonde, waar de commandanten van deze onderdelen elkaar vlot moeten kunnen vinden om bij meldingen te overleggen wie de meest logische behandelaar is. Dit beeld hebben wij opgenomen in het gesuggereerde stroomschema.

- Met het oog op de zwaardere rol dient COID te worden uitgebreid. In omvang maar ook in de beschikbare competenties en ervaring. Het gaat onder meer om juridische expertise, maar ook om medewerkers van voldoende niveau die de triage kunnen doen bij binnenkomende vragen: is advies aan de leidinggevende nodig? Welk advies kan de medewerker die zich bij ons meldt het beste krijgen? Wie moet in elk geval worden geïnformeerd?

7 Tot slot: bodem bereikt?

Terug naar het begin. Het verzoek aan ons was om diepgaand onderzoek te doen, tot op de bodem. Eerdere onderzoeken hadden weinig concrete aanwijzingen opgeleverd dat er zaken mis waren, maar de signalen bleven terugkomen. Ook op politiek niveau. Wij hebben een jaar lang grondig onderzoek gedaan. Betekent dit dat we alles hebben gehoord en gezien? Waarschijnlijk niet. Maar wij hebben al het mogelijke gedaan om mensen hun verhaal te laten doen. En wij onderzochten de aangedragen casuïstiek. Daaruit komt niet het beeld naar voren dat er zaken hebben plaatsgevonden als corruptie, omkoping, fraude, daadwerkelijke belangenverstrengeling of het te eigen bate misbruiken of manipuleren van informatie. Wij concludeerden dat in het verleden niet alles volgens de regels is verlopen. Wij concludeerden ook dat het integriteitsbeleid, functiescheiding in aanbestedingen en aandacht voor leiderschap hun vruchten wel af lijken te werpen. En wij deden in het vorige hoofdstuk aanbevelingen om enkele aanpassingen te doen om integriteitsrisico's te verminderen en om meldingen van vermoedens van misstanden beter te kunnen behandelen. Hier gaat het natuurlijk primair om het gedragsrepertoire van onder andere leidinggevenden. Maar ook om de middelen en de methoden die hen daarbij helpen.

Hebben wij de bodem bereikt? Nee. Onze voornaamste conclusie is juist – en dat drong pas gaandeweg het onderzoek tot ons door - dat de bodem nooit bereikt is. Onder onderzoek als dit valt nooit een streep te zetten. Praten over integriteit, over vermoedens die je hebt, over vragen die je hebt, over dingen die je ziet: het moet altijd doorgaan. Juist daarom is onze belangrijkste aanbeveling aan het ministerie om in beweging te blijven met integriteit. Menigeen zal wellicht denken: "wat een softe aanbeveling na al die forse verhalen over integriteitschendingen en onregelmatigheden, hadden ze niet wat duidelijker kunnen zijn?" Wij zijn echter van mening dat elke nieuwe regel die we zouden hebben bedacht, af zou leiden van waar het werkelijk om gaat: neem de onderliggende oorzaken weg die leiden tot het steeds opkomen én voortbestaan van vermoedens van belangenverstrengeling. Alleen dan kan je moreel fit worden en blijven.

Net als bij gewone fitness vergt ook *moral fitness* dagelijkse oefeningen. Dat stelt hoge eisen aan leidinggevenden. Vragen van medewerkers moeten worden beantwoord. Communicatie over aanstaande veranderingen moet transparant, ruimhartig en empathisch zijn. Signalen moeten altijd aanleiding zijn tot actie. Praat erover en koppel op. Dat geldt eens te meer bij terugkerende of aanhoudende signalen. En die actie kan geen dichotoom onderzoek zijn naar de vraag of regelgeving wel of niet is gevolgd. De belangrijke spelers moeten snel om tafel om de vraag te beantwoorden: "Wat is hier nu eigenlijk aan de hand?" Besef dat het antwoord hierop nooit zwart/wit zal zijn. En vervolgens: "Wat gaan we doen om dit op te lossen?"

> ***"In accordance with physical fitness, moral fitness is also a process; there is no farthest point toward which it works, but it is a continuous effort to improve the performances of the past. For this reason, moral fitness requires dialogue and debate, openness and transparency, integrity and a willingness to correct oneself."***
> (bron: '*Moral fitness for peace operations*', R. Richardson, D. Verweij en D. Winslow)

MORAL FITNESS FOR PEACE OPERATIONS

DR. R. RICHARDSON
DR. D. VERWEIJ
PROF. DR. D. WINSLOW
Royal Netherlands Military Academy
Free University of Amsterdam

Journal of Political and Military Sociology, 2004, Vol. 32, No. 1 (Summer):99-113

"Moral Fitness" refers to an attitude of alertness and responsibility on a moral level. In light of the fall of Srebrenica, we show that moral fitness is an important attitude in military-operations-other-than-war to deal with moral dilemmas. These operations and the dilemmas that follow differ fundamentally in their dominating elements from war-fighting operations due to our so-called "risk society." We conceive of "moral fitness" in reference to ethics in the present day and past (Aristotelian) context, and discuss the analogy with "physical fitness" to show its capacity to be trained. In the end we focus on responsibility and accountability as the two pillars of moral fitness in the light of the cases in Srebrenica and Rwanda.

INTRODUCTION

At the turn of the 20th Century, people predicted an era of peace and prosperity for the coming 100 years. Nevertheless, we found ourselves engaged in vast blood letting conflicts that no one could have imagined at that time. It is difficult to guess what the future holds, but we can be certain that the faces of war and peace will change dramatically. As a result, we think that the new leadership challenges will put greater demands upon military personnel than ever before.

In particular, we believe that the scale, complexity, and scope of operations of operating systems and technology in military operations-other-than-war are leveraging moral dilemmas in new ways. Future operations will be much more complex and will require more ethical sophistication. In this article we introduce the term "moral fitness" as an answer to this required sophistication, after discussing the features and context of modern military operations-other-than-war. We also discuss the added value of "moral fitness" in dealing with ethical dilemmas in these operations. To be morally fit implies a state of self- reflective "being" rather than a series of prescriptions about behavior.

In order to examine this concept of "moral fitness" more closely, we will be using a concrete example from the Dutch peacekeeping experience in Srebrenica. Thus, we begin the article with a description of the case study of Srebrenica and some of the moral dilemmas soldiers encountered. We then go

on to discuss the future face of peace operations and what they can mean to ethical decision making in a military context. This is followed by a more theoretical discussion of what we mean by "moral fitness" and an exposé of our ideas concerning accountability and responsibility. At the end, we will make some concluding remarks and refer to future developments of the concept of moral fitness.

SREBRENICA: A CASE STUDY

Let's have a short look at the operation of DUTCHBAT3[1] in Srebrenica[2] in order to introduce the complexity of the peace operations environment. The Dutch became involved in the peacekeeping efforts in the Balkan war at an early stage. The Dutch sent observers, a Communications Battalion, and a Transport and Logistics Battalion in 1992. During 1993, discussions centered on the matter of sending a *combat* unit. Initially, both the Minister of Defense and the Army Staff had strong reservations about the risks and usefulness of deploying a combat unit to a country that was still caught in a major civil war. Also, the Dutch Armed Forces were in the process of large-scale reductions and reorganization following the 1993 "Defense Priorities Review." However, these concerns were put aside by the Parliament, the press, and public opinion, all who demanded quick and decisive humanitarian intervention in the Bosnian war. This interventionism was strongly fueled by very disturbing pictures from death-camps in Bosnia. In the autumn of 1993, the Minister of Defense conceded: that a battalion from the new Airmobile Brigade ("red berets") would be sent to Bosnia. This deployment was supposed to bolster the Owen-Stoltenberg Peace Plan, but this plan soon failed. The battalion was then incorporated in "safe areas" policy. Early in 1994 the first airmobile battalion was sent to the isolated Muslim safe area of Srebrenica in Eastern Bosnia. The Dutch Government made it clear that it would end this deployment after 18 months (i.e., rotations of personnel on 6-month tours).

The first battalion immediately encountered insurmountable political and operational problems. These increased even more as the second and third battalions were deployed. The mandate was vague. Were the Dutch airmobile soldiers supposed to actually defend the 40,000 or so strong Muslim population

---

[1] Some parts of this section are drawn from an article by D. Winslow and C. Klep (1999) "Besmeurde erfenis. Het onderzoek naar wangedrag van Canadese para's in Somalie." (Dishonoured Legacy; Research into the Canadian Airborne's Mission to Somalia) *Militaire Spectator*, 2: 89-97.

[2] The enclave Screbrenica, a Muslim enclave in Boxnia Herzegovina, was meant to be protected by a Dutch Battalion (DUTCHBAT). The Third rotation of that battalion, DUTCHBAT3, was present in the enclave during the Bosnic Servian attack July 6-21, 1995.

against a Bosnian Serb attack? Or was their presence one of a "trip wire," the crossing of which would spark off large scale North Atlantic Treaty organization intervention (mainly from the air)? Also, the Bosnian Serbs increased their stranglehold on the enclave, blocking resupply convoys and preventing new personnel and journalists from reaching the enclave. Meanwhile, little attention was given to the plight of the airmobile soldiers in their native country, much to their chagrin.

In the summer of 1995, the tables were finally turning against the Bosnian Serbs on the battlefield. Apparently, as part of a last all-out offensive, the troops of general Mladic systematically reduced the Eastern-Bosnian enclaves of Gorazde, Zepa, and Srebrenica. After some initial skirmishes, the Bosnian Serb troops overran the "safe area" of Srebrenica in an operation that lasted less than two days (July 11and 12). The battalion counted on air support to repel the attack, but the United Nations and NATO proved reluctant. In the immediate aftermath of their successful attack, the Serbs rounded up the Muslim women, children, and elderly and evacuated them to Muslim territory. However, an estimated 5,000-7,000 men were massacred in the vicinity of the enclave. The battalion spent another week in the now deserted enclave before being allowed by the Bosnian Serb leadership to return to Zagreb and to an elated welcome in the Netherlands.

Media frenzy in the Netherlands erupted during and immediately after the arrival of DUTCHBAT3 in Zagreb on July 22, 1995, ten days after the fall of "safe area" Srebrenica, and the subsequent return of the main body of the Dutch battalion to the Netherlands two days later. The elation about their safe return changed into severe criticism literally overnight as stories from refugees of Srebrenica began to come out. Public debate then focused upon the stickier moral question of whether the Dutch peacekeepers should have protected the inhabitants of the enclave from ethnic cleansing and mass killings, despite their limited resources.

Some fundamental issues concerning this question are found in the *Debriefing Report of Srebrenica.* The Debriefing report, written in 1999, tries to give a "complete as possible overview of the events and to give an overview of the connections between several events in Srebrenica in the period from 6-12 July 1995" (Debriefing Report Screbrenica 1999:1). This was done analyzing 451 debriefings with DUTCHBAT3 soldiers who were in Srebrenica during the downfall of this enclave in July 1995. The research findings show a remarkable pattern of military conduct in this operation.

First of all, the Report indicates that a great number of soldiers, regardless of rank, were confronted with mass media attention. These soldiers were interviewed by the written press (local, regional, and national), as well as by several foreign and domestic television stations. On most occasions, soldiers became aware of the difficulty of judging their statements and anticipating the

consequences of statements that they made to the press (Debriefing Report Screbrenica 1999:8-12).

Secondly, the Debriefing Report shows that negotiation was, in several important stages of decision-making, carried out in direct contact with the combatant parties on the battalion level but also on the lowest platoon level. An example of such negotiations occurred during the fall of the enclave when even low ranking officers had to confront the question of the triage of 239 Muslim men (Debriefing Report Screbrenica 1999:15). Thirdly, the Report describes 168 occasions when military personnel were sometimes threatened with death and/or forced to hand over their weapons and equipment to the combatant parties (Debriefing Report Screbrenica 1999:18-19).

In addition, military personnel in several compounds were engaged in bartering with locals; they exchanged equipment and food for liquor and food, but they also traded food, money, and tobacco for sex (Debriefing Report Screbrenica 1999:26-27). Also on many occasions, locals who regularly visited the military compounds stole UN equipment, and soldiers were offered money or other favors to smuggle letters or money abroad (Debriefing Report Screbrenica 1999:19-25). Some incidents of sex, alcohol, drugs, and racial misconduct internally and towards locals were also mentioned in the Debriefing Report (Debriefing Report Screbrenica 1999:26-31,36-43, 50-51).

Finally, on many occasions, the mandate of DUTCHBAT3 was shown to be insufficient. For example the instruction to "disarm the combatants" could never be executed because of the lack of military personnel and equipment on the occasions heavily armed combatant groups were spotted or encountered.[3] Therefore, in situations of danger, it was not always possible to execute orders given by higher-level commands and headquarters (Debriefing Report Screbrenica 1999:56-57). This caused great frustration and annoyance at the Non Commissioned Officer (NCO) and Non Commissioned Member (NCM) level. Furthermore, the communication between the different levels of command was troublesome. Because communication with headquarters was troublesome, personnel were forced to sometimes make decisions on their own (Debriefing Report Screbrenica 1999:55, 65-66).

Previously, we illustrated a number of situations that could have created moral dilemmas in military conduct in the specific peace operation of Srebrenica. The question is how to deal with these dilemmas in such new military operations-other than-war? How are soldiers and officers prepared to confront them? Can the concept of moral fitness aid them in preparing for these challenges?

---

[3] The Debriefing Report even mentioned that military personnel said that: "This mandate (the defense of the enclave Screbrenica) should have been executed by two battalions instead of one."

FEATURES OF FUTURE OPERATIONS

The challenges faced in Srebrenica serve as an example of modern peacekeeping operations. Although it is doubtful that Dutch forces will ever be involved in the protection of a safe haven/enclave again, peace operations will most likely remain the major Dutch military activity (Defense Note 2000). The features of these operations differ fundamentally from war-fighting operations (see list below). In military operations-other-than-war, new societal values come to the fore. Today, people are not willing to sacrifice the lives of their children in unpopular wars; thus, it is more difficult to bring body bags home. Likewise, people have a more enlightened attitude about appropriate treatment of "the enemy," so military personnel are now expected to deal respectfully with other cultures.

The most important features of peacekeeping operations in comparison with war-fighting operations include:

- Multinational operations (UN operations);
- Operations in built up or urban areas (for example, the Srebrenica enclave);
- Post conflict reconstruction and nation building;
- Multiple players such as humanitarian relief agencies, NGOs, multilateral organizations, political actors, military forces, etc.;
- Cultural diversity among the multiple players;
- Lack of strategic direction;
- Decentralized diplomacy (i.e., decision making and negotiating) by relatively young and sometimes inexperienced military personnel who now need to be able to dialogue with new actors (combatant and non combatant);
- Media intensity;
- Individuals accountable for their decisions and actions;
- Military personnel responsible for a wider range of activities;
- Lack of (or limited) rule of law;
- Restrictive rules of engagement, especially concerning the use of weapons.

Offense, unity of command, maneuver, and surprise remain the dominant elements of war operations while restraint and principles of unity of effort among a variety of actors dominate peace operations. In its complexity, peace operations like Srebrenica are also characterized by an *expanded scope* concerning the actors involved (NGOs, national governments, international agencies etc.) as well as *increased fragmentation* (more complex at lower levels concerning actions and decisions). In short, not only are the rules of military operations changing, but the game is also shifting.

THE CONTEXT OF FUTURE OPERATIONS

The shifting game of military operations in the 21st century must be understood in the context of social, technical, and economic developments in our society. On the macro level, these developments can best be described in terms of *reflexive modernization* (Beck 1992). As a result of technological and scientific progress, society changes fundamentally: "Modernization *within* the paths of industrial society is replaced by modernization *of the principles* of industrial society" (Beck 1992:10). During this process, people are disentangled from their old political-democratic and social-cultural bonding, and are confronted with new ones. Two mechanisms appear at the same time in this "Janus-face" process of reflexive modernization, *globalization* and *individualization* (particularization) (Beck 1992).[4] The result of both mechanisms is a society which can best be characterized as a *risk society* that goes from managing one crisis to the next without addressing the root causes of its problems (Beck 1992). In this risky context, future military operations change fundamentally. Situations and responsibility become ambiguous and fuzzy. It becomes difficult to anticipate the effects of one's actions or inactions. An important question for the military in these circumstances of permanent change and uncertainty is the question of how to deal with moral issues. This is because the factors mentioned above imply an increase of moral issues and dilemmas within military operations. Bauman (1998) shows us that in this society of permanent change, pluralism of values, and uncertainty, more or less straight moral standards or rules will be absent. Every person will, in these circumstances, continuously make choices and will therefore take responsibilities on his/her own. This will not lead to moral anarchy or disintegration as pessimists will argue, but to new moral challenges and an authentic responsibility. People will no longer push off moral choices and responsibilities to a higher authority, but address them on their own (Bauman 1998). It is important to remember that this moral complexity is not static, but arises in response to the intricacy of the options faced. Therefore, we want to introduce a dynamic view seizing upon the trend in military organizations to reflect upon lessons learned in peace operations, particularly by elaborating the concept of moral fitness.

---

[4] Also see A Giddens (1992) *Modernityand Self-Identity.* Cambridge: Polity Press and Z. Bauman (1998) "Postmoderne moraliteit" (Postmodern Morality) in R. Munters (1998) *Leven met veranderlijkheid. Verscheidenheid en onzekerheid.* Amsterdam: Boom (pp. 105-115).

WHAT DO WE MEAN BY MORAL FITNESS?

In order to explain the term "moral fitness" we will first say something about ethics and ethical questions and dilemmas. By doing this we will be able to portray the context in which the term "moral fitness" functions.

The consideration of ethical questions and dilemmas in a risk society has so far led to the production of codes of conduct for an increasing number of professions, including the military. As these codes of conduct seem to have the function of a panacea rather than a set of values that people actually live by,[5] the question is whether this is the right answer for future ethical questions and dilemmas. In different fields of applied ethics, the metaphor of the pyramid of ethics can be used to indicate what ethics is actually about and what the problems are (Dullaert 1999). This notion of the pyramid of ethics is based on a definition of ethics that consists of several links, or, to put it in another way, a definition of ethics that consists of several layers that are connected. In the following figure, words that are in Italics point to underlying concepts.

Ethics:	reflection on and explication of *morality*
Morality:	*norms* and *values* of a certain group of people in a certain period
Norm:	rule, a guideline to act upon; norms are based on *values*
Value:	an ideal, something you strive for, a conviction or principle; values for the foundation of ethics

Figure 1: Ethics Pyramid

This layered definition can be compared to a pyramid of which the top is formed by ethics (reflection) and the basis or foundation is formed by the

[5] A code of conduct seems to be a panacea, a universal remedy, against the problems that occur – and the number of problems is legion. More and more codes of conduct for more and more professions arise. These codes seem to have the function of an incantation, as they are often called into being when it is observed that the things that are not supposed to happen, happen continually. D.Verweij (2000) "Moed: mythe of morele kwaliteit?" (Courage: Myth or Moral Quality?) In *Militaire Spectator*, jaargang 169 nr. 2.

values (ideals, convictions, or principles). This metaphor of the pyramid points out that the building of ethics needs a solid foundation, for a foundation is of crucial importance to what is placed on top of it. It is clear that foundation problems have consequences for the rest of the building: the walls sag, the roof falls in, and eventually the building is uninhabitable. Thus, if ethics cannot rest on and is not formed by the awareness of concrete values, "ethics" as such is an empty concept and ineffective in practice. Both on a theoretical and practical level, ethics can only be made meaningful by stimulating the awareness of values. This sounds easier than it is because values are relative. Values do not have the same meaning to all people in comparable situations. Our multiform society illustrates that what is valuable to one person is without value to the other, yet the starting point for any ethics program and for moral education lies in making people aware of the values (personal and social) that are at stake in the situation one finds oneself in.

Verweij (2000) has pointed out that it seems that, in our day and age, this pyramid of ethics has fallen apart. The top of the pyramid seems to have tumbled town, which means that the connection between the top and the foundation of the pyramid no longer exists. In other words ethical reflection is no longer anchored in the practice of values people are aware of and actually live by. On the contrary, ethical reflection seems to be detached from the practice of values. Moreover, there seems to exist a multitude of values (the former foundation of the pyramid) on which there is no reflection whatsoever. The lack of reflection turns these values into free-floating values that to some people are not recognizable as values and to others seem unimportant because it is not evident what the meaning and consequences of these values are (since meaning and consequences can only be made clear by reflection).

The effect of all this is that, on the one hand, we live in a society in which there is a lot of talk about, and lots of policies on, ethics. However, these talks about ethics and these ethical policies are not attuned to the practices of those values that people are aware of and actually live by. On the other hand, the practices around us consist of a multitude of values that are often not recognized as such and that are mostly non-committal and volatile. In both cases, the absence of actual commitment and engagement is striking. The result of this is that, on the one hand, there are policies, especially codes of conduct, that are implemented in corporations from the top and about which employees shrug their shoulders and do nothing. On the other hand, this results in the homage to certain values, if it happens to be convenient, without any thought about the actual meaning of these values or their consequences. Real reflection is missing.

What holds for ethics in general holds for applied ethics as well. With reference to the military, this means that it is important that a policy is not just put on paper but rooted in the attitude of military personnel of all ranks. In this respect, one can ask questions about the way the code of conduct for the Dutch Army was implemented. After a more or less failed implementation a few years

ago, someone came up with the idea to put every code at the bottom of a picture in which a certain sports event is shown. These pictures decorate the walls of military institutions. That is about all they do, for the effect of these silent and meager contributions to moral education seems shallow.

THE ANALOGY BETWEEN PHYSICAL FITNESS AND MORAL FITNESS

Education and training play an important role in moral development. However, how can the effect of training and education be measured? Straight A's for ethic tests and papers are no guarantee for morally just behavior. Moreover, morally just behavior is not something that is only tested once. It is something that needs to be displayed whenever it is required, and the circumstances that require this behavior have to be identified as such by the person who has to display the behavior. Because of this necessary omnipresence of the knowledge of, and the ability to display, morally just behavior in circumstances that require this behavior, we would like to introduce the term "moral fitness." In other words, we consider "moral fitness" an adequate term because it refers to the necessary alertness and responsibility on a moral level. Being morally fit seems the only guarantee that in confrontation with moral dilemmas one can make a morally responsible decision.

In order to explain the term "moral fitness" in more detail, we would like to draw attention to the analogy that exists between physical fitness and moral fitness. Like physical fitness, moral fitness also implies regular training in order to stay in shape. Moral fitness is not something that can be won once and for all; it requires a continuous reflection on the values and norms one lives by and is confronted with, reflection on what to do and how and why it should be done. If one is morally fit or in good shape, one has to stay that way.

As with physical fitness, moral fitness also requires checks and evaluations to ascertain one's fitness. This implies that there are standards one has to meet. As with physical fitness, these standards are not just one's own standards. Although the fitness of persons differs, and fitness has an irrefutable subjective aspect, there are more or less objective standards one has to live up to in order to be called "fit." In this respect, it is important to ascertain who decides what the standards of moral fitness are. Also, there is the necessity to make sure there are no double standards. Everyone has to be subjected to the same moral test.

In accordance with physical fitness, moral fitness is also a process; there is no farthest point toward which it works, but it is a continuous effort to improve the performances of the past. For this reason, moral fitness requires dialogue and debate, openness and transparency, integrity and a willingness to correct oneself.

MORAL FITNESS: A "CLASSICAL" CONCEPT

Moral fitness is an appropriate term for the moral attitude that is needed in our post-modern time. It points to the attitude of a person who can cope with an increase in ethical questions and dilemmas because he or she has the necessary moral alertness required. Moral fitness implies that a person regularly practices self-critical reflection.

However post-modern "moral fitness" may be, it is related to the ethical tradition of the past. To be more precise, it is related to Aristotelian ethics. Moral fitness emerges from what Aristotle called "phronesis" and "virtue." "Phronesis" can be translated as "practical insight" or "practical wisdom." Aristotle defines "virtue" as a state of character concerned with choice. It is practical wisdom that makes it possible to make the right choice, the choice that lies in a mean between two vices, that which depends on excess and that which depends on defect. Virtue is the ability to choose the "right mean." This is a disposition that is acquired by habit. Aristotle states that "moral virtue comes about as a result of habit, whence also its name (ethike) is one that is formed by a slight variation from the word 'ethos' (habit)" (Aristotle 1997).

Aristotle explains the term "right mean" by stating that there are certain qualities that can be nullified both by defect and by excess. This holds for instance for physical power and health. Too much as well as too little physical training affects physical power. In a similar way, both excess and defect of food and drink corrode health. Only the "right mean" results in physical power and health. One of the examples Aristotle discusses is "courage" as the right mean between fear and recklessness. Correspondingly, every virtue is the ability to find the "right mean." This "right mean" is always the right mean in relation to us, Aristotle states. He illustrates the meaning of this statement with the example of the amount of meat an athlete should eat. If ten pounds of meat is considered much and two pounds is considered little, the mean is six pounds. However, Aristotle points out, a trainer will not, without due consideration, prescribe this mean to every athlete. He will have to determine the right amount for every individual. In other words, finding the right mean demands that people find their own right mean.

The term "moral fitness" fits the Aristotelian framework. Firstly, Aristotle uses the analogy of physical concepts to explain moral concepts like, for instance, physical power and health, physical training and the amount of food athletes eat. Secondly, according to Aristotle, virtue has to be demonstrated in action. In other words, virtues have to be put into practice. Thirdly, Aristotle explicitly states that virtue is a state of character that can be acquired by habit. In other words, one has to work on it. Fourthly, virtues have a subjective, but also an objective aspect. Aristotle discusses the mean in relation to us, but the ability to choose this mean requires practical wisdom.

On the basis of Aristotle's ethics, "moral fitness" can be described as having practical wisdom. This means that one is able to find the right mean between two extreme positions. This illustrates one's virtues. Virtues contribute to a good and flourishing life. At the end of the *Ethica Nicomacheia*, Aristotle points to the *Politica*, his book on politics, which he considers a continuation of his book on ethics. To Aristotle, ethics and politics are connected. That is understandable because Aristotle is convinced that a flourishing life, the realization of which is discussed in the *Ethica Nicomacheia*, can only be fully realized in a political community, a *polis*. What connects the members of a polis is a shared ideal of a good and flourishing life. The political community is the place where virtues can grow. Thus, a community of persons can foster moral fitness among its members. For the military community, this means a thorough understanding, application, and practice of the principles of accountability and responsibility.

ACCOUNTABILITY AND RESPONSIBILITY

In our opinion, moral fitness for the military must be grounded in accountability and responsibility, which are twin pillars upholding the functioning of the military in a free and democratic society. Accountability is a vexing concept for theorists across a broad range of disciplines. It is often ill defined and erroneously merged with the allied concept of responsibility. Accountability is the mechanism for ensuring conformity to standards of action. In the military, this means that those called upon to exercise substantial power and discretionary authority must be answerable (i.e., subject to scrutiny, interrogation and, ultimately, commendation or sanction) for all activities assigned or entrusted to them. In any properly functioning system or organization, there should be accountability for actions, whether those actions are executed properly and lead to a successful result or are carried out improperly and produce injurious consequences.

In peace operations, even though military personnel are technically accountable to their immediate superiors in the chain of command, media intensity can focus public attention. This then leads to public scrutiny. Thus soldiers and officers may find themselves called to account for their actions (or inaction) before civilian inquiries, civilian authorities, and/or the public via the media (Dishonoured Legacy 1997).

The term responsibility is not synonymous with accountability. One who is authorized to act or exercises authority is "responsible." Responsible officials are held to account. An individual who exercises powers while acting in the discharge of official functions is responsible for the proper exercise of the powers or duties assigned. As mentioned above, in peace operations there are a wide range of responsibilities. Military personnel may become responsible for

the well being of the host population and for a wide delivery of services from protection to humanitarian relief.

Let's have a closer look at the terms accountability and responsibility in relation to the military. When an officer accepts command of troops, he/she accepts not only the responsibility of accomplishing a mission but also the guardianship of those who serve under his or her command. However, this is not always possible. In Srebrenica, DUTCHBAT was not given the resources (e.g., manpower, air support, supplies) to accomplish its mission. In fact, there were so few resources available to DUTCHBAT that protection of the enclave was considered a "mission impossible." In addition, commanders can be torn between the guardianship of those under their command and those they are there to protect. Here the concept of responsibility becomes fuzzy indeed. If we accept that Lt. Col. Karremans was responsible for the safety of his troops, then allowing them to stand aside in the face of overwhelming Serb firepower makes sense. However, if responsibility for the safety of the citizens of the enclave is paramount, then standing aside may not be the morally fit response. One can say that Lt. Col. Karremans was an effective commander because he brought all his men and women home safely. However, one can also ask the question whether it was morally fit to accept gifts from and make a toast with someone (Bosnian Serb General Mladic) under whose command thousands of innocent people were massacred (NOVA 1999).

Finally it is important to remember that the chain of accountability and responsibility extends beyond the level of the military. In peace operations, there are international agencies such as the UN and many national governments involved. They must also be held accountable for acting responsibly. Should they also be held accountable for the failure to take action? (e.g., Karremans called in air strikes but they came too late to save the enclave). The question then arises, "accountable to whom?" and "responsible for what?" In a risk society, the management of public perceptions and political interests often seems to take precedence in answering the question.

Moral fitness for a military commander not only means a thorough understanding of accountability and responsibility, and with that understanding come difficult choices. Let us consider the circumstances of Canadian General Tousignant, who was Force Commander of the United Nations' Assistance Mission in Rwanda from 1994 to 1996. General Tousignant was facing a situation of over 1½ million internally displaced persons when the Government of Kigali ordered all refugee camps to be closed. As the camps began to close, refugees fled to the other camps until they converged on the final remaining camp at Kibeho. When General Tousignant consulted with UN in New York concerning the possibility that the government would want to close the camp by force he was told to pull out of Kibeho. However, General Tousignant could not in his own conscience abandon the women and children in the camp. When the massacre at Kibeho began in April of 1995, he did not pull out his Zambian

battalion. Less than 4,000 Rwandese were killed, but thousands of other lives were saved by the military presence. General Tousignant writes:

> Rationalizing a decision not to follow directions from UN Headquarters on a moral issue does not in any way remove the question of ethical dilemma and certainly does not relieve the Commander of his responsibilities towards his superiors. Not to execute a lawful command is rarely justifiable and it is clear that I defied an order from New York at Kibeho. (Tousignant 1996:35)

Even though he was responsible for the safety of his battalion, General Tousignant let the safety of the camp refugees be paramount and thus put the troops under his command at risk. Fortunately for his career no soldier was killed:

> I was never asked to account for my decision and the fact that none of my soldiers was killed probably contributed to making this difference of opinion a non-issue. (Tousignant 1996:35)

CONCLUSIONS

Operations-other-than-war differ from military operations of the 20th century in scope and execution. If current trends continue, future military operations, especially operations-other-than-war, will be more complex than ever. Part of this complexity is the increase in moral dilemmas faced by military personnel. We introduced the term "moral fitness" as an appropriate term for the moral attitude that is needed to confront the moral questions and dilemmas that will be faced by future military operations. Moral fitness points to the attitude of a person who can cope with the increase of these questions and dilemmas, because he or she has the necessary moral alertness that is required.

Moral fitness is a dynamic, not a static concept. It requires the ability to demonstrate the appropriate attitude in the appropriate situation. Moral fitness also requires checks and evaluations to ascertain one's fitness. Moral fitness is a process; it is a continuous effort to improve the performance of the past. All this implies that striving for moral fitness requires the ability to reflect upon oneself. Therefore, it requires dialogue and debate, openness and transparency, integrity and a willingness to correct oneself.

Moral fitness fits into an Aristotelian framework and as such it is also related to Virtue Ethics, an ethical theory that finds general favor nowadays (Statman 1997). This popularity is related to the focus of Virtue Ethics on the individual and personal character and the relation of the individual to others and to society. Virtue ethics is not about abstract rules and programs that are implemented from the top-down into a community. The community itself encourages moral fitness by fostering principles such as accountability and responsibility. For the military community, being accountable means that

soldiers appearing in future military operations will always be subject to scrutiny from their superiors as well as from the public (and the media!). They must be able to answer for their actions. Responsibility means that soldiers in future operations must be aware of their tasks and the wide range of possible impacts their actions will have during the execution of these tasks. This applies not only to the military but also to the international agencies that take part in the chain of responsibility and accountability.

Organizations involved in future peace operations (such as the military, NGOs, the media, and international organizations) must have well-developed self-diagnostic capabilities, allowing them to question their governing assumptions and reassess their relationship to changing environmental demands (i.e., peace operations). In this way, organizations "learn how to learn" by maintaining processes that critically examine key assumptions, beliefs, tasks, decisions, and structural issues (Purser & Pasmore 1992). Weick and Westley (1996) tell us that such systems need to have the "institutionalization of doubt" (i.e., questioning). "Self-designing systems apply the lessons of the past while simultaneously questioning their relevance" (Weick & Westley 1996:444).

In operations of the future, soldiers will often be alone in small groups in different cultural circumstances. They must be morally fit in order to prevent a breakdown of discipline and control during the operation. The same holds for the organizational level. Thorough procedures must exist to prevent and fight outbursts of disciplinary and moral breakdowns during and after the operation. Thus, moral fitness is a synergy concept involving individuals, groups, and organizations. The presence of moral fitness on several levels is a necessary condition for the effectiveness of ethics.

REFERENCES

Aristotle
1997 *Ethica Nicomacheia.* Translated and elucidated by C. Hupperts and B. Poortman. Amsterdam: Kalias.

Bauman, Z.
1998 "Postmoderne moraliteit" (Postmodern Morality). In R. Munter (ed.) *Leven met veranderlijkheid, verscheidenheid en onzekerheid* (pp. 105-115). Amsterdam: Boom.

Beck, W.
1992 *Risk Society: Towards a New Modernity.* London: Sage.

Minister of Public Works
1997 *Dishonoured Legacy.* Commission of Inquiry into the Deployment of Canadian Forces to Somalia. Ottawa: Minister of Public Works.

Giddens, A.
1992 *Modernity and Self-Identity.* Cambridge: Polity Press.

Ministerie van Defensie
1999 *Feitenrelaas Debriefing Screbrenica* (Debriefing Report Screbrenica). Den Haag: Ministerie van Defensie.

Ministerie van Defensie
1999 *Defensie nota 2000* (Defense Note 2000) Den Haag: Ministerie van Defensie, Directie voorlichting.

NOVA
1999 "A Cry from the Grave" (Documentary).

Purser, R. E., and W. A. Pasmore
1992 "Organization for Learning." In W. A. Pasmore & R. W. Woodman (eds.) *Research in Organizational Change and Development* (Vol. 6, p. 55). Greenwich, CT: JAI Press.

Statman, D.
1997 *Virtue Ethics: A Critical Reader*. Edinburgh: Edinburgh University Press.

Tousignant, G.
1996 *Ethical Dilemmas of Commanders on Operational Missions: Four Views*. Ottawa: Department of National Defense.

Verweij, D.
2000 "Moed: mythe of morele kwaliteit?" (Courage: Myth or Moral Quality?). *Militaire Spectator*, jaargang 169 nr. 2.

Verweij, D. and C. Dullaert
1999 "Aristoteles en de rechter-bemiddelaar" (Aristotle and the Judge-Mediator). In *Trema, tijdschrift voor de rechterlijke macht* (p. 8). Deventer: Tjeenk Willink.

Weick, K. E., and F. Westley
1996 "Organizational Learning: Affirming an Oxymoron." *Handbook of Organization Studies*: 444

Winslow, D., and C. Klep
1999 "Besmeurde erfenis. Het onderzoek naar wangedrag van Canadese para's in Somalie" (Dishonoured Legacy: Research into the Canadian Airborne's Mission to Somalia) *Militaire Spectator*, 2:89-97.

Dit is een uitgave van:

ABDTOPConsult
Postbus 20011
2500 EA Den Haag

abdtc@minbzk.nl
www.algemenebestuursdienst.nl